PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04L 9/08, H04Q 7/38** — **A1**

(11) International Publication Number: **WO 97/45981**

(43) International Publication Date: 4 December 1997 (04.12.97)

(21) International Application Number: PCT/GB97/01407

(22) International Filing Date: 23 May 1997 (23.05.97)

(30) Priority Data:
9611411.1 31 May 1996 (31.05.96) GB

(71) Applicant *(for all designated States except US)*: ICO SERVICES LTD. [GB/GB]; 1 Queen Caroline Street, London W6 9BN (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: JOHNSTON, Thomas, Francis [CA/GB]; 22A Cleveland Square, London W2 6DG (GB).

(74) Agents: READ, Matthew, Charles et al.; Venner, Shipley & Co., 20 Little Britain, London EC1A 7DH (GB).

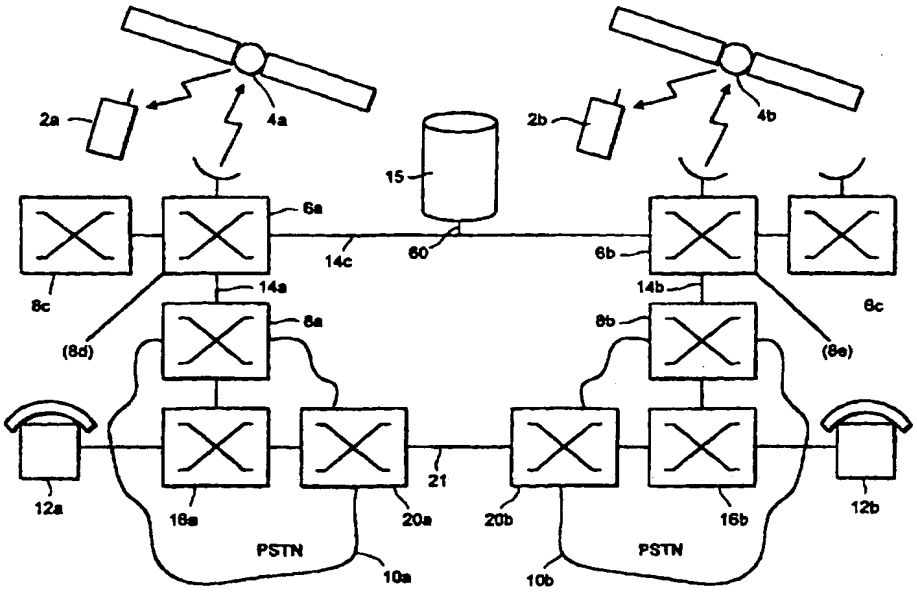
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE COMMUNICATION



(57) Abstract

A method of distributing through a communications network enciphering keys for a secure communications session via said network between first and second terminals (2a, 2b) corresponding first and second terminal keys (K_a, K_b) comprising: storing said first and second terminal keys (K_a, K_b) remotely to said terminals (2a, 2b); providing a number (RAND); generating first and second corresponding partial keys (K_{pa}, K_{pb}) each comprising a corresponding function of said number (RAND) and a corresponding one of said terminal keys (K_a, K_b); and dispatching the first partial key (K_{pa}) towards the second terminal (2b), and vice versa.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURE COMMUNICATION

This invention relates to a method and apparatus for secure communications.

Digital mobile voice communications systems are known. One example is the GSM terrestrial cellular system; others are the Inmarsat-M satellite telephone system, the IRIDIUM (TM) satellite cellular system (described in, for example, EP-A-0365885), the ICO (TM) satellite cellular system (described in, for example, GB-A-2295296) or the ODYSSEY (TM) satellite cellular system (described in, for example, EP-A-0510789).

Since such systems operate over a wireless link, there is a risk of interception of calls by unauthorised persons.

The GSM system includes an optional encryption scheme described in, for example, "Security aspects and the implementation in the GSM-system"; Peter C.J. van der Arend, paper 4a, Conference Proceedings of the Digital Cellular Radio Conference (DCRC), October 12th-14th 1988, published by Deutsche Bundespost, France Telecom and Fernuniversitate. Greater detail is given in the following GSM recommendations:

GSM 02.09 "Security Aspects"; GSM 03.20 "Security Related Network Functions"; GSM 03.21 "Security Related Algorithms".

In this scheme, a database known as the Authentication Centre (AuC) holds an individual encryption key number (K_i) for each subscriber to the authentication service, which is also stored on a chip known as the Subscriber Information Module (SIM) held in the subscriber's mobile terminal. The subscriber has no access to the data stored in the SIM and cannot read the key.

Where a secure session is requested, a random number (RAND) is generated by the Authentication Centre and used, together with the customer's key (K_i), to calculate a ciphering key (K_c) used during the session for ciphering and deciphering messages to/from the subscriber.

The random number is sent to the subscriber's mobile terminal via the Base Transceiver Station (BTS). The mobile terminal passes the random number to the SIM, which calculates the ciphering key K_c using an algorithm termed A5.

Thus, the random number is sent over the air, but not the customer's key K_i or the ciphering key K_c.

The random number and the ciphering key K_c are sent to the Home Location Register (HLR) database storing details for the subscriber concerned and are also sent to the Visiting Location Register (VLR) for the area where the use is currently located, and are supplied to the BTS via which the mobile is communicating.

The ciphering key K_c is used, together with the current TDMA frame number, to implement the A5 ciphering algorithm in the mobile terminal and the Base Transceiver Station. Thus, the individual user key K_i is stored only at the authentication centre and the SIM, where the ciphering key K_c is calculated and forwarded to the BTS and the mobile terminal.

Whilst this scheme is adequate in many respects, it fails to provide complete security since it offers protection only over the air transmission path. Thus, it is possible for illicit access to be obtained by tampering with the fixed part of the network.

Accordingly, the present invention provides a mobile communications system utilising end-to-end encryption. Because the encryption runs from one user

terminal to the other, across the whole communications path and not just the air path, improved privacy is obtained.

The basic problem in offering end-to-end encipherment of communications over a network is in providing each of the two users with the same, or each other's, secret key.

In some applications, a group of terminals (for example all owned by a single body) may all have access to the same key. Whilst this provides privacy against personnel from outside the group, it is an incomplete solution since it does not provide privacy for communication between two terminals within the group and a third within the group.

It is possible to employ public key encryption systems, in which each terminal has a secret decryption key and a non-secret encryption key, so that any other party can use the encryption key to encrypt data but only the recipient can decrypt data which has been encrypted using the public encryption key.

A communication system could be envisaged in which every user is provided with such a pair of keys, and in setting up a communication between a pair of users each sends the other its encryption key whilst keeping its decryption key secret.

However, there is widespread public concern that the use of such techniques on a telecommunications network would allow criminals or terrorists to communicate using completely secure communications, free from any possibility of supervision.

Accordingly, aspects of the present invention may provide of a "trusted third party" database holding copies of the keys, and distributing to each terminal key data relevant to the key of the other terminal.

Preferably, the key data sent to each terminal is masked, to prevent its interception by an eavesdropper and very preferably, even the receiving terminal is unable to extract or recover the key of the terminal. Instead, in a preferred embodiment, each terminal constructs a key dependent jointly upon its own key and the key data received in relation to the other terminal.

In a preferred embodiment, the masking takes the form of processing each terminal key together with a number (the number being the same for each terminal key) using a function so that, although neither terminal can extract the other terminal's key, each can construct the same combination of the two keys and the number as an enciphering key.

The invention is envisaged for use in satellite mobile digital communications systems, and is also useful in corresponding terrestrial digital mobile communication systems (e.g. in cellular systems such as the GSM system), or in fixed link communication systems. The invention may also be practised in store-and-forward communication systems such as e-mail or the Internet.

Aspects of the invention and preferred embodiments thereof are described in the claims and the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram showing schematically the elements of a communications system embodying the present invention;

Figure 2 is a block diagram showing schematically the elements of mobile terminal equipment suitable for

use with the present invention;

Figure 3 is a block diagram showing schematically the elements of an Earth station node forming part of the embodiment of Figure 1;

Figure 4 is a block diagram showing schematically the elements of a gateway station forming part of the embodiment of Figure 1;

Figure 5 is a block diagram showing schematically the elements of a database station forming part of the embodiment of Figure 1;

Figure 6 illustrates the contents of a store forming part of the database station of Figure 5;

Figure 7a illustrates schematically the beams produced by a satellite in the embodiment of Figure 1;

Figure 7b illustrates schematically the disposition of satellites forming part of Figure 1 in orbits around the earth;

Figure 8 is a block diagram showing the signal flow between components of the handset of Figure 2 in a first embodiment of the invention;

Figure 9 is a schematic block diagram showing the flow of encryption data and signals between the components of Figure 1 in the first embodiment;

Figure 10a is a flow diagram showing schematically the process performed by the control and enciphering components of the handset of Figure 8 in the first embodiment;

Figure 10b is a flow diagram showing schematically the process of operation of the earth station of Figure 3 in the first embodiment;

Figure 10c is a flow diagram showing schematically the process of operation of the central database station of Figure 4 in the first embodiment;

Figure 10d is a flow diagram showing schematically the process of operation of a subscriber

information module (SIM) held within the handset of Figure 8 in the first embodiment;

Figure 11a is a an illustrative diagram showing the stages of formation of the enciphering key by a first handset terminal of Figure 8; and

Figure 11b is a corresponding illustrative diagram showing the process of formation of the enciphering key at a second such handset;

Figure 12 is a flow diagram modifying the operation of that of Figure 10c in a third embodiment of the invention;

Figure 13b is a flow diagram modifying the operation of that of Figure 10d in the third embodiment;

Figure 14 is a flow diagram illustrating schematically the stages of security provided in a fourth embodiment of the invention;

Figure 15a is a block diagram showing schematically some of the functional elements present in the handset of Figure 8 according to the fourth embodiment of the invention;

Figure 15b is a block diagram showing schematically some of the functional elements present in the database station of the fourth embodiment;

Figure 15c is a block diagram showing schematically some of the functional elements present in the earth station of the fourth embodiment;

Figure 16a (incorporating parts of Figure 10a) is a flow diagram showing schematically the operation of a handset according to the fourth embodiment;

Figure 16b (incorporating parts of Figure 10b) is a flow diagram showing schematically the process of operation of an earth station according to the fourth embodiment;

Figure 16c (incorporating parts of Figure 10c) is

a flow diagram showing schematically the operation of a database station according to the fourth embodiment; and

Figure 16d (incorporating parts of Figure 10d) is a flow diagram showing schematically the operation of a subscriber information module according to the fourth embodiment.

PREFERRED EMBODIMENT

Referring to Figure 1, a satellite communications network according to this embodiment comprises mobile user terminal equipment 2a,2b; orbiting relay satellites 4a,4b; satellite earth station nodes 6a,6b; satellite system gateway stations 8a,8b; public switched telecommunications networks 10a,10b; and fixed telecommunications terminal equipment 12a,12b.

Interconnecting the satellite system gateways 8a,8b with the earth station nodes 6a,6b, and interconnecting the nodes 6a,6b with each other, is a dedicated ground-based network comprising channels 14a,14b,14c. The satellites 4, earth station nodes 6 and lines 14 make up the infrastructure of the satellite communications network, for communication with the mobile terminals 2, and accessible through the gateway stations 8.

A terminal location database station 15 is connected, via a signalling link 60 (e.g. within the channels 14 of the dedicated network) to the gateway station and earth stations 6.

The PSTNs 10a,10b comprise, typically, local exchanges 16a,16b to which the fixed terminal equipment 12a,12b is connected via local loops 18a,18b; and international switching centres 20a,20b connectable one to another via transnational links 21 (for example, satellite links or subsea optical fibre cable links). The PSTNs 10a,10b and fixed terminal

equipment 12a,12b (e.g. telephone instruments) are well known and almost universally available today.

Each mobile terminal apparatus is in communication with a satellite 4 via a full duplex channel (in this embodiment) comprising a down link channel and an up link channel, for example (in each case) a TDMA time slot on a particular frequency allocated on initiation of a call, as disclosed in UK patent applications GB 2288913 and GB 2293725. The satellites 4 in this embodiment are non geostationary, and thus, periodically, there is hand over from one satellite 4 to another.

Mobile terminal 2

Referring to Figure 2, the mobile terminal equipment of Figure 1 is shown.

One suitable form is a handset, as shown. Details of the handsets 2a,2b etc do not form part of the present invention, but they may comprise handsets similar to those presently available for use with the GSM system, comprising a digital coder/decoder 30, together with conventional microphone 36, loudspeaker 34, battery 40 and keypad components 38, and a radio frequency (RF) interface 32 and antenna 31 suitable for satellite communications. Preferably a display 39 (for example a liquid crystal display) is also provided. A 'smart card' reader 33 receiving a smart card (SIM) 35 storing user information is also provided.

The coder/decoder (codec) 30 comprises a low bit rate coder, generating a speech bit stream at around 3.6 kilobits per second, together with a channel coder applying error correcting encoding, to generate an encoded bit stream at a rate of 4.8 kilobits per second. The low bit rate coder may, for example, be a linear predictive coder such as a multiple pulse

predictive coder (MPLPC) a code book excited linear predictive coder (CELP), or a residual excited linear predictive coder (RELP). Alternatively, it may employ some form of waveform coding such as subband coding.

The error protection encoding applied may employ block codes, BCH codes, Reed-Solomon codes, turbo codes or convolutional codes. The codec 30 likewise comprises a corresponding channel decoder (e.g. using Viterbi or soft decision coding) and speech decoder.

Also provided is a control circuit 37 (which may in practice be integrated with the coder 30) consisting of a suitably programmed microprocessor, microcontroller or digital signal processor (DSP) chip.

The SIM 35 preferably complies with GSM Recommendations 02.17 "Subscriber Identity Modules", and 11.11 and is preferably implemented as an industry standard "Smart Card". The SIM 35 and reader 33 are therefore preferably as described in International Standards ISO 7810, 7811 and 7816; these and GSM 02.17 and 11.11 are all incorporated herein by reference.

Specifically, the SIM 35 includes a processor 35a and permanent memory 35b. The processor 35a is arranged to perform some encryption functions as described in greater detail below.

Earth Station Node 6

The earth station nodes 6 are arranged for communication with the satellites.

Each earth station node 6 comprises, as shown in Figure 3, a conventional satellite earth station 22 consisting of at least one satellite tracking antenna 24 arranged to track at least one moving satellite 4, RF power amplifiers 26a for supplying a signal to the antenna 24, and 26b for receiving a signal from the antenna 24; and a control unit 28 for storing the

satellite ephemeris data, controlling the steering of the antenna 24, and effecting any control of the satellite 4 that may be required (by signalling via the antenna 24 to the satellite 4).

The earth station node 6 further comprises a mobile satellite switching centre 42 comprising a network switch 44 connected to the trunk links 14 forming part of the dedicated network. A multiplexer 46 is arranged to receive switched calls from the switch 44 and multiplex them into a composite signal for supply to the amplifier 26 via a low bit-rate voice codec 50. Finally, the earth station node 6 comprises a local store 48 storing details of each mobile terminal equipment 2a within the area served by the satellite 4 with which the nodes 6 is in communication.

Gateway 8

Referring to Figure 4, the gateway stations 8a,8b comprise, in this embodiment, commercially available mobile switch centres (MSCs) of the type used in digital mobile cellular radio systems such as GSM systems. They could alternatively comprise a part of an international or other exchange forming one of the PSTNs 10a,10b operating under software control to interconnect the networks 10 with the satellite system trunk lines 14.

The gateway stations 8 comprise a switch 70 arranged to interconnect incoming PSTN lines from the PSTN 10 with dedicated service lines 14 connected to one or more Earth station nodes 6, under control of a control unit 72. The control unit 72 is capable of communicating with the data channel 60 connected to the database station 15 via a signalling unit 74, and is arranged to generate data messages in some suitable format (e.g. as packets or ATM cells).

Also provided in the gateway stations 8 is a store 76 storing billing, service and other information relating to those mobile terminals 2 for which the gateway station 8 is the home gateway station. Data is written to the store 76 by the control unit 72 after being received via the signalling unit 74 or switch 70, from the PSTN 10 or the Earth station nodes 6 making up the satellite network. This store acts in the manner of a visiting location register (VLR) of a terrestrial GSM network, and a commercially available VLR may therefore be used as the store 76.

The satellite system trunk lines 14 comprise, in this embodiment, high quality leased lines meeting acceptable minimum criteria for signal degradation and delay. In this embodiment, all the lines 14 comprise terrestrial links. The trunk lines 14 are preferably dedicated lines, so that the lines 14 form a separate set of physical channels to the networks 10. However, the use of virtual circuits through the networks 10 is not excluded.

Database Station 15

Referring to Figure 5 the database station 15 comprises a digital data store 54, a signalling circuit 56, a processor 58 interconnected with the signalling circuit 56 and the store 54, and a signalling link 60 interconnecting the database station 15 with the gateway stations 8 and Earth stations 6 making up satellite system network, for signalling or data message communications.

The store 54 contains, for every subscriber terminal apparatus 2, a record showing the identity (e.g. the International Mobile Subscriber Identity or IMSI); the current status of the terminal 2 (whether it is "local" or "global" as will be disclosed in

greater detail below); the geographical position of the mobile terminal 2 (either in co-ordinate geometry, or as code identifying an area within which it lies); the "home" gateway station 8 with which the apparatus is registered (to enable billing and other data to be collected at a single point) and the currently active Earth station node 6 with which the apparatus 2 is in communication via the satellite 4. The contents of the store are indicated in Figure 6.

Further, in this embodiment the store contains for each user a unique and individual enciphering key K_i, to be used as described below.

The signalling unit 56 and processor are arranged to receive interrogating data messages, via the signalling circuit 60 (which may be a packet switched connection), from gateways 8 or nodes 6, comprising data identifying one of the mobile terminals 2 (for example, the telephone number of the equipment 2), and the processor 58 is arranged to search the store 54 for the status and active earth station node 6 of the terminal 2 and to transmit these in a reply message via the data line 60.

Thus, in this embodiment the database station 15 acts to fulfil the functions both of a home location register (HLR) of a GSM system, and of an authentication centre (AuC) of a GSM system, and may be based on commercially available GSM products.

Satellites 4

The satellites 4a,4b comprise generally conventional communications satellites, such as the known Hughes HS 601 model, and may be as disclosed in GB 2288913. Each satellite 4 is arranged to generate an array of beams covering a footprint beneath the satellite, each beam including a number of different frequency channels and time slots, as described in

GB 2293725 and illustrated in Figure 7a.

The satellites 4a are arranged in a constellation in sufficient numbers and suitable orbits to cover a substantial area of the globe (preferably to give global coverage) for example 10 (or more) satellites may be provided in two (or more) mutually orthogonal intermediate circular orbits at an altitude of, for example, 10,500 kilometres as shown in Figure 7b. Equally, however, larger numbers of lower satellites may be used, as disclosed in EP 0365885, or other publications relating to the Iridium system, for example.

Registration and Location

In one embodiment, a customer mobile terminal apparatus 2 may be registered with one of two distinct statuses; "local" in which the mobile terminal apparatus is permitted only to communicate through one local area, or part of the satellite system network, and "global", which entitles the apparatus to communicate through any part of the satellite system network.

The status of each apparatus 2 (i.e. "local" or "global") is stored in the record held for the apparatus 2 concerned in the store 54 of the database station 15.

The mobile terminal apparatus 2 performs an automatic registration process, of the kind well known in the art of cellular terrestrial communications, on each occasion when the terminal 2 is utilised for an outgoing call; and/or when the apparatus 2 is switched on; and/or periodically whilst the apparatus 2 is switched on. As is conventional, the registration process takes the form of the broadcasting of a signal identifying the mobile terminal 2 (e.g. by transmitting its telephone number on a common hailing

or signalling frequency).

The transmitted signal is picked up by one or more satellites 4. Under normal circumstances, the signal is picked up by multiple satellites 4, and the received signal strength and/or time of arrival are transmitted, together with the identity of the mobile apparatus 2 and of the satellite 4 receiving the signal, to the database station 15 via the earth stations node or nodes 6 for which the satellites 4 are in communications, and the signalling line 60.

The processor 58 of the database station 15 then calculates, e.g. on the basis of the differential arrival times, the terrestrial position of the mobile terminal apparatus 2, which is stored in the database 54. Also stored is the identity of the earth station node 6 most suitable for communicating with the mobile terminal apparatus 2 (the "active" station). This is typically found by the processor 58 comparing the stored position of the terminal 2 with the predetermined stored positions of each of the earth station nodes 6 and selecting the nearest. However, account may also or instead be taken of the strength of the signals received via the satellites 4, or of other factors (such as network congestion) to result, in borderline cases, in the choice of a node earth station which is not geographically closest to the mobile terminal equipment 2. The identity of the allocated active earth station node 6 is then likewise stored in the store 54 in the record for that terminal apparatus.

CALL SET UP AND ROUTING

The processes of routing calls to and from mobile terminal apparatus 2 are described fully in GB-A-2295296 or PCT/GB95/01087, both of which are hereby incorporated fully by reference. Briefly, for

a local user outside its area, a call placed to the user or from the user is referred to the database station which determines that the user is outside of its area and thereafter does not process the call. For a local user which is inside its area, in the preferred embodiment described in the above referenced British and International application, calls to or from the user are set up over the satellite link, via the active earth station 6, the ground network, and the international public switch telephone network (PSTN) from the nearest gateway 8 to the terrestrial user.

For global users, calls are routed via the satellite and the active earth station, then via the ground network to the gateway station 8 nearest to the terrestrial user.

The dial numbers allocated to mobile users may have "International" prefixes followed by a code corresponding to the satellite service network. Alternatively, they could have a national prefix followed by a regional code assigned to the satellite service.

Calls between one mobile user and another are carried out by directing the signal via a first satellite link down to the active earth station node of the first mobile user, via the ground network to the active earth station node of the second mobile user (which may be, but is not necessarily, the same as that of the first) and then via a second satellite link (which may, but does not need to be via the same satellite) to the second mobile user.

FIRST EMBODIMENT

Figure 8 shows in greater detail the signal flow through the elements of the mobile terminal of Figure 2. Signals received from the ariel 31 are RF

demodulated by RF modem 32 and supplied to the processor circuit 37 which is arranged, when in enciphering mode, to decipher the received data using, for example, the A5 algorithm in accordance with a deciphering key supplied from the SIM 35. The deciphering key is referred to as $K_{a,b}$.

The deciphered bit stream is then passed to a channel codec 30b which performs error correcting decoding and the error corrected speech signal is supplied to low bit rate codec 30a which includes a digital to analog converter, the analog output of which is supplied to loudspeaker 34.

Speech from the microphone 36 is supplied to the low bit rate codec 30a which includes an analog to digital converter, and the resulting low bit rate speech signal is encoded by the channel codec 30b to include error protection. The error protected bit stream is then encrypted, when in enciphering mode, by the control circuit 37 and the encrypted bit stream is supplied to the RF modem 32 for transmission from the aerial 31.

Referring to Figures 9, 10 and 11, the process of setting up the enciphered mode of communication will now be described in greater detail.

During a communication session between two user terminals 2a,2b, a user of one or both terminals elects to continue the conversation in encrypted form. Accordingly, referring to Figure 10a, in step 1002 the invoking party enters a sequence of key strokes from the keyboard 38 which is recognised by the processor 37 as an instruction to invoke security and accordingly the processor 37 transmits, in step 1002, a signal to invoke enciphering on an inband or associated control channel.

Referring to Figure 10b, at the earth station 6,

in step 1102 the privacy request signal is received and in step 1104 the signal is sent in parallel to the central database station 15 (with the identity codes indicating the identities of the terminals 2a and 2b) and to the second user terminal 2b.

At the second user terminal 2b, receipt of the privacy signal occurs in step 1002 of Figure 10a.

Referring to Figure 10c, at the central database station the privacy signal is received in step 1202.

In step 1204, the controller 58 of the database station 15 accesses the memory 54 and reads out the individual enciphering key K_a stored for the first mobile terminal 2a, and the key K_b stored for the second mobile terminal 2b.

In step 1206, the controller 58 generates a pseudo random number (RAND).

In this embodiment, the keys K_a and K_b are each 128 bit binary numbers and the random number RAND is another 128 bit binary number.

In step 1208, the controller 58 calculates first and second partial keys K_{pa}, K_{pb}. The calculation of the second partial key is illustrated in Figure 11a; this calculation comprises generating a 128 bit number each bit of which comprises the exclusive OR function of the bits in corresponding positions of the second terminal key K_b and the random number RAND. Thus, the second partial key K_{pb} is equal to K_b + RAND (where + indicates the exclusive-OR operation for binary numbers).

The first partial key K_{pa} is calculated in exactly the same way, by performing a bit-wise exclusive-OR operation between the first terminal key K_a and the random number RAND, as shown in Figure 10b.

In step 1210, the central database station 15 transmits the first partial key (K_{pa}), to the second

terminal 2b and the second partial key (K_{pb}) to the first terminal 2a, via the signalling network 60, and the respective earth stations 6b and 6a and satellites 4b and 4a.

At this stage, each individual terminal key has been "scrambled" by the exclusive OR operation with the random number RAND. An unauthorised eavesdropper who monitors one of the partial keys cannot learn the terminal key from it from because he faces two unknowns; the random number RAND and the terminal key. Even an unauthorised eavesdropper who monitors both partial keys cannot derive either the random number or one of the terminal keys, because he has only two data from which to derive three unknowns; the best that can be derived is the difference between the two terminal keys, which is of no value.

Referring now to Figure 10b, in step 1106 each earth station receives the partial key and forwards it to the mobile terminal in step 1108.

Referring to Figure 10a, in step 1004, each of the mobile terminals receives a corresponding partial key. In step 1006, the partial key is transmitted via the card reader 33 to the SIM 35.

Referring to Figure 10d, in step 1302, the SIM receives the partial key and in step 1304 the SIM reads the terminal key from within the memory 35b. In step 1306, the SIM processor 35a calculates the enciphering key, by performing a bit wise exclusive-OR operation between the received partial key and the stored terminal key to generate a new 128 bit binary number. In step 1308, the SIM 35 supplies the enciphering key thus calculated (termed $K_{a,b}$) via the card reader device 33 to the terminal processor 37.

It will be recalled that the partial key supplied to the first terminal 2a comprised the product of an

exclusive-OR function between the terminal key K_b of the second terminal 2b and the random number RAND ($K_{pb}=K_b+RAND$). Thus, as shown in Figure 10a, the enciphering key calculated in step 1306, as the product of an exclusive-OR operation between this partial key K_{pb} and the terminal key K_a, is $K_{ab}=K_b+RAND+K_a$.

Likewise, at the second terminal 2b, as shown in Figure 10b, the enciphering key K_{ab} calculated is the product of the exclusive-OR operation between the partial key K_{pa} and the terminal key K_b; in other words, $K_{ab}=K_a+RAND+K_b$.

Since the exclusive-OR operation obeys the associative law of mathematics, these two results are identical; in other words, each terminal calculates the same enciphering key.

Referring back to Figure 10a, in step 1008 the terminal processor 37 receives the encryption key K_{ab} and in step 1010 the terminal 37 switches to encryption mode. Thereafter, as shown in step 1012, the processor 37 functions to encrypt the bit stream from the codec 30 prior to RF modulation and transmission, and to decrypt the corresponding bit stream from the RF modem 32 prior to supply thereof to the codec 30.

The encryption algorithm may be any suitable algorithm and may be openly known (since the encryption key itself is secret). In particular, conveniently the encryption algorithm is the A5 encryption algorithm used in GSM handsets and described in the above referenced Recommendations; this is already present in most GSM handsets.

Thus, to recap, as shown in Figure 9, in this embodiment each terminal 2 has an associated unique terminal key which is stored in the SIM 35 held within

the terminal and in the central database station 15. The enciphering key used is a function of both terminal keys. The database station 15 distributes to one terminal 2 the terminal key of the other terminal.

The terminal keys are distributed in masked form. The masking in this embodiment takes the form of an exclusive-OR operation with a random number. The operation performed at each terminal to combine its own terminal key with the other, masked, terminal key results in each terminal producing an encrypted terminal key which is the same function of both terminal keys. This is conveniently arranged in this embodiment by processing each terminal key in accordance with the same terminal number.

Transmitting the terminal keys in masked form prevents an eavesdropper from gaining access to either terminal key. By changing the masking on each session operation (e.g. by generating a continually changing sequence of pseudo-random numbers) an eavesdropper cannot learn the masking function over time.

Nor is it possible for either terminal or SIM to work out the other's terminal key, since this is masked even from the terminals themselves.

Finally, as in GSM systems, neither terminal knows its own terminal key, because it is stored on the SIM, to which access is denied from the terminal. This is important since, otherwise, one terminal could in principle listen to the partial key sent to the other terminal and, knowing its own terminal key, derive the random number from which it could then decipher the other terminal key from the partial key transmitted to it.

SECOND EMBODIMENT

In a second embodiment, security is further improved by reducing the opportunities for

unauthorised tampering at the central database station. The second embodiment works substantially as the first except that, as shown in Figure 11, instead of steps 1204 to 1210 of Figure 10c being performed, steps 1404 to 1420 are performed.

Accordingly, after step 1202, the processor 58 first accesses the first terminal key K_a in step 1404; then calculates the random number in step 1406 (as described above in relation to step 1206); then calculates the first partial key in step 1408 (as described above in relation to step 1208); then sends the first partial key in step 1410 (as described above in relation to step 1210).

After these operations, any locally stored copies of K_a and K_{pa} are erased. Then, in step 1414, the processor 58 accesses the second terminal key K_b, calculates the second partial key (step 1416); sends the second partial key (step 1418); and erases the second partial key and second terminal key (step 1420).

Thus, in this embodiment, access to the two partial keys and terminal keys is separated in time, reducing the possibilities for eavesdropping or fraudulent use of the database station 15.

It will be apparent that access to the two partial keys and/or terminal keys could be separated in other manners; for example, by sending the two terminal keys to physically separate devices and then sending the random number to each of the devices for combination there with the terminal keys.

Rather than sending the same random number to two different devices, for additional security, two identical, in-step, random number generators may be provided at two different locations, to which the two terminal keys are sent. Thus, access to the two

terminal keys and/or partial keys may be separated physically as well as, or instead of, in time.

THIRD EMBODIMENT

In the above embodiments, the partial keys K_{pa}, K_{pb} are transmitted en clair. In this embodiment, securing is further increased by enciphering each for transmission.

Although it would be possible to use a common cipher, this would be undesirable since eavesdroppers with access to the common cipher (e.g. other authorised users of the privacy service) might be able to decipher the cipher.

Equally, it is preferred not to use an air interface cipher of the type known in the GSM system because this would be open to interception in the fixed part of the network.

Accordingly, in this embodiment, the SIM 35 stores a decryption algorithm (which may conveniently be the A5 algorithm used in GSM systems) and the database station 15 is arranged to execute the corresponding encryption algorithm.

Referring to Figure 13a, in this embodiment the process of Figure 10c of the first embodiment is modified by the inclusion of a step 1209, between steps 1208 and 1210, in which each partial key is enciphered using the terminal key of the terminal to which it will be sent and is transmitted in enciphered form.

At each terminal, referring to Figure 13b, in this embodiment the SIM processor 35a performs an additional step 1305 between steps 1304 and 1306. In step 1305, the received partial key is decrypted using the terminal key, prior to calculating the ciphering key.

Thus, in this embodiment, additional security is

provided by encrypting the transmitted partial keys; particular conveniently, the encryption makes use of the terminal key of the destination terminal, so to avoid the need to store further encryption data.

Obviously, however, other forms of encryption are possible; in particular, more sophisticated encryption algorithms in which an additional random number is also sent would be possible.

Finally, it may be mentioned that where the encryption scheme described in this embodiment is used, it would be possible to directly encrypt the transmitted terminal keys, rather than partial keys formed by masking the terminal keys. This should still offer good security in most circumstances, since only in the SIM 35 are the received terminal keys deciphered. However, where there is a risk that fraudulent SIMs might be manufactured then masking to produce a partial key will be employed since this conceals even from the SIM the identity of the other terminal key.

FOURTH EMBODIMENT

In this embodiment, the principle of the first embodiment is utilised, in combination with the air interface encipherment and authentication system present in GSM compatible networks and specified in the above GSM recommendations.

Referring to Figure 14, the security features are applied in the following order:

Authentication (step 2002); Air-Interface encryption (step 2004); End-to-End encryption (step 2006).

Essentially, the first two steps are as in existing GSM networks and the third is as described above as in relation to the first embodiment. However, for the sake of clarity, further description

will be given hereafter.

Referring to Figure 15a, the functions performed by the handset processor 37 and SIM 35 will be described as separate functional blocks; each functional block could, of course, be implemented by a separate microprocessor or digital signal processor (DSP) device but in this embodiment, in fact, only one such processor device is present in the handset and one in the SAN 35.

Referring to Figure 15a, signals received from the antenna 31 and demodulated by the RF modem 32 are passed through a first enciphering/deciphering stage 372 arranged to apply the A5 algorithm known from GSM in accordance with an air interface enciphering key K_c, and a second enciphering/deciphering stage 374 arranged to apply a second deciphering algorithm (conveniently, again, the A5 algorithm used in the GSM system and described in the above Recommendations) deciphering in accordance with an end-to-end enciphering key $K_{a,b}$. The deciphered bit stream is thereafter supplied to the codec 30.

Similarly, the speech bit stream from the codec 30 passes through the two enciphering/deciphering stages 372,374 in the reverse order; for clarity, the signal path has been omitted from Figure 15a.

Within the SIM 35 is located a terminal key storage register 352 storing the terminal key K_i for the terminal. The terminal key storage register 352 is connected to supply the terminal key K_i to a signature calculation stage 354, arranged to calculate a "signed response" number (SRES) used to authenticate the terminal, in accordance with the A3 algorithm described in the above mentioned GSM Recommendations and used in GSM systems. The response calculation stage 354 is also connected, via the card reader

device 33, to receive a random number (RAND1) from the unenciphered bit stream output from the RF modem 32.

The terminal key register 352 is also connected to supply the terminal key K_i to a first key generation stage 356, which is also arranged to receive the random number (RAND 1) and to calculate therefrom an air interface enciphering key K_c in accordance with the A8 algorithm described in the above GSM Recommendations and used in GSM systems. The key thus calculated is supplied, via the card reader device 33, to the first (air interface) enciphering/deciphering stage 372 of the terminal processor 37.

The terminal key register 352 is also connected to supply the terminal key to a second key generation stage 358, which is arranged to generate an enciphering key K_{ab} for end-to-end encryption (as described in the first embodiment above) utilising the terminal key K_i and the partial key K_{pb} which it is connected to receive (via the card reader device 33) from the deciphered output of the first (air interface) enciphering/deciphering stage 372 of the terminal processor 37.

The end-to-end enciphering key thus calculated is supplied to the second (end-to-end) enciphering/ deciphering stage 374 of the terminal processor 37.

Referring to Figure 15b, the central database station comprises, in this embodiment, a random number generator 582 arranged to generate, on each occasion of use, a new binary 128 bit number (RAND1) in a random sequence; a store 54 storing the terminal keys K_i; a key generation stage 584 which is connected to receive a terminal key from the store 54, and the random number (RAND1), and to calculate therefrom an air interface enciphering key K_c in accordance with the A8 algorithm (described in the above GSM

recommendations and used in GSM systems); and a signature calculation stage 586, which likewise is connected to receive the terminal key and the random number, arranged to calculate the signed response number (SRES) in accordance with the A3 algorithm (described in the above mentioned GSM Recommendation and used in GSM systems).

The outputs of the random number generator stage 582, signed response generator stage 586 and key generation stage 584 are connected to the signalling circuit 56 for transmission to the earth stations 6.

Referring to Figure 15c, each earth station 6 comprises (within the database 48) a triplet register 482 arranged to store a predetermined number (e.g. 5) of triplets each comprising a random number, a corresponding signed response (SRES) and a corresponding air interface encryption key (K_c), supplied via the signalling circuit 60 from the database station 15.

On each occasion when a mobile terminal 2 registers with the earth station 6, the earth station requests the supply of the predetermined number of triplets from the central database station 15, which accordingly generates the predetermined number of triplets and transmits them for storage in the registers 482 via signalling channel 60.

Also provided within the earth station 6 is a comparator 282 coupled to the triplet register 482 and to the air interface components 24, 26 of the earth station 6, and arranged to compare a signed response (SRES) number received from a mobile terminal 2 with a signed response stored in the register 482, and to indicate correspondence (or absence thereof) between the two numbers. If the two numbers do not correspond, the user is not authenticated and service

is discontinued by the control unit 28.

Finally, the earth station 6 comprises an air interface encryption stage 284 arranged to encipher and decipher in accordance with the A5 algorithm (known from GSM) making use of an air interface enciphering key K_c supplied from the triplet register 482.

In the enciphering direction, the air interface enciphering/deciphering stage 284 receives an input from the codec 50 and delivers its output to the air interface components 24,26; whereas in the deciphering direction the enciphering/deciphering stage 284 receives its input from the air interface components 24, 26 and delivers its output to the codec 50.

The operation of this embodiment will now be described in greater detail with reference to Figures 16a to 16d. In Figures 16a to 16d, steps of the processes of Figure 10a to 10d, which will not be discussed further in detail, are incorporated.

As in Figure 10a, a request for privacy is initiated by one of the parties and a privacy request signal is transmitted from the terminal 2a.

Following receipt (step 1102) of the privacy signal at the earth station 6a and forwarding thereof (step 1104) to the database station 15, referring to Figure 16c, steps 1202 and 1204 are performed to derive the terminal keys of the two terminals.

Then, in step 1205, a test is performed to determine whether both subscribers are authorised to use end-to-end encryption. If so, steps 1206 to 1210 of Figure 10c are performed. Subsequently, or if not, the database station 15 proceeds to step 1212, in which it transmits a signal to the earth station(s) 6a,6b serving the two terminals 2a,2b to instruct them to perform a terminal authentication check and to

commence air interface encryption.

Referring back to Figure 16b, each earth station 6, on receipt of the instruction signal and partial key (step 1110), sends an authentication interrogation message (step 1112) which includes the next random number RAND1 obtained from the triplet register 482. Additionally, as in the GSM system, a key number may be transmitted for further verification.

Referring back to Figure 16a, on receipt of the authentication request message (step 1014) the random number (RAND1) is extracted and sent to the SIM 35 (step 1016).

Referring to Figure 16d, at the SIM 35, on receipt of the random number RAND1 (step 1310), the SIM processor 35a looks up the terminal key K_a, (step 1312) and calculates the signed response (SRES) using the A3 algorithm (step 1314).

In step 1316, the SIM processor 35a calculates the air interface enciphering key K_c using the random number (RAND1) and the terminal key K_a. In step 1318, the SIM 35 transmits the signed response number (SRES) and the air interface enciphering key (K_c) to the terminal processor 37 via the card reader device 33.

Subsequently, the SIM 35 executes the process of Figure 10d.

Referring to Figure 16a, on receipt of the signed response number (SRES) in step 1018, the terminal processor 37 transmits the SRES number to the earth station 6a (step 1020).

Referring to Figure 16b, the earth station 6 receives the signed response number (1114) and compares it with the stored signed response number held in the triplet register 482 (step 1116).

If the two do not match, then the call is terminated (step 1117). Alternatively, further

attempts at authentication may be made if desired.

If the signed response received from the mobile terminal 2 matches the stored signed response in step 1116, the earth station 6 reads the enciphering key K_c stored in the triplet register 482 corresponding to the signed response just received, and (step 1118) commences enciphering all future traffic to, and deciphering all future traffic from, the mobile terminal 2 using the A5 algorithm together with the enciphering key K_c. As is conventional in GSM systems, the frame number may also be used as an input to the enciphering algorithm.

The earth station 6 thereafter returns to step 1108 of Figure 10c, to send the partial key received from the database station 15 to the terminal 2, but in this embodiment this takes place in enciphered form.

Returning to Figure 16a, on receipt of the air interface encryption key K_c (step 1022) from the SIM 35, the terminal processor 37 starts the enciphering/deciphering mode in which all traffic received from the air interface modem 32 is deciphered and all traffic transmitted to the air interface modem 32 is enciphered using the A5 algorithm and the air interface enciphering key K_c; where the earth station 6 additionally makes use of the frame number, the terminal 2 likewise does so.

The process performed by the terminal processor 37 then returns to step 1004 of Figure 10a, to receive (in encrypted form), decrypt and use the partial enciphering key K_{pb} received from the earth station 6.

Although the above description assumes that neither terminal has recently been authenticated, and that neither terminal is already in air interface encryption mode, it will be understood that this need not be the case. If either terminal is already

applying air interface encryption, then the corresponding steps described above to set up authentication and air interface enciphering are not performed again.

In the above embodiment, additional safeguards may be provided; for example, to initiate secure communications, the terminal user may be required to input a PIN code for matching with data held on the SIM.

It will be understood that, where the invention is practised in a GSM-compatible system or the like, the SIM 35 will contain further information in the form of the international mobile subscriber identity number (IMSI), and optionally lists of phone numbers for speed dial or other purposes.

The invention is conveniently practised by maintaining lists at the database station 15, each of which specifies the members of a corresponding closed user group (CUG). Members of one closed user group are thereby permitted to correspond with other members of the same user group. For example, closed user groups might comprise armed services personnel of different countries; or emergency services personnel of different countries.

OTHER EMBODIMENTS

It will be clear from the foregoing that the above described embodiment is merely one way of putting the invention into effect. Many other alternatives will be apparent to the skilled person and are within the scope of the present invention.

For example, the numbers of satellites and satellite orbits indicated are purely exemplary. Smaller numbers of geostationary satellites, or satellites in higher altitude orbits, could be used; or larger numbers of low earth orbit (LEO) satellites

could be used. Equally, different numbers of satellites in intermediate orbits could be used.

Although TDMA has been mentioned as suitable access protocol, the present invention is fully applicable to other access protocols, such as code division multiple access (CDMA) or frequency division multiple access (FDMA).

Whilst the principles of the present invention are envisaged above as being applied to satellite communication systems, the use of the invention in other communications systems (e.g. digital terrestrial cellular systems such as GSM) is also possible.

Although, for the sake of convenience, the term "mobile" has been used in the foregoing description to denote the terminals 2, it should be understood that this term is not restricted to hand-held or hand-portable terminals, but includes, for example, terminals to be mounted on marine vessels or aircraft, or in terrestrial vehicles. Equally, it is possible to practice the invention with some of the terminals 2 being completely immobile.

Instead of providing a single central database station 15 storing details of all terminal equipment 2, similar details could be stored at the home gateway 8 for all terminal equipment to register with that home gateway 8.

Equally, whilst in the above described embodiments the central database station 15 acts as a Home Location Register (HLR) of a GSM system, and may be provided using commercially available HLR hardware, and the databases within each earth station 6 act in the manner of visiting location registers (VLRs) and may likewise use commercially available GSM hardware, it will be understood that the information relating to

different users could be distributed between several different databases. There could, for instance, be one database for each closed user group, at physically different positions.

Whilst in the fourth embodiment above the same terminal key K_i is used for secure end-to-end encryption as is used for air interface encryption, it will be clear that this is not necessary; each terminal could store two different terminal keys, one for air interface encryption and one for end-to-end encryption. In this case, a separate authentication centre database could be provided for end-to-end encryption key distribution to that which is used in conventional air interface encryption.

Although in the foregoing embodiments, the same (A5) cipher algorithm used for the air interface encryption of the GSM system is proposed for use in end-to-end encryption, it will be apparent that a different cipher could be used; in this case, terminals would include two different enciphering stages for use in the fourth embodiment. Further, where multiple closed user groups are provided, each closed user group could use a different cipher.

In the foregoing, the gateways 8 may in fact be comprised within an ISC or exchange or mobile switching centre (MSC) by providing additional operating control programmes performing the function of the gateway.

In the foregoing, dedicated ground networks lines have been described, and are preferred. However, use of PSTN or PLMN links is not excluded where, for example, leased lines are unavailable or where temporary additional capacity is required to cope with traffic conditions.

It will naturally be clear that the stores within

the gateways 8 need not be physically co-located with other components thereof, provided they are connected via a signalling link.

Whilst, in the foregoing, the term "global" is used, and it is preferred that the satellite system should cover all or a substantial part of the globe, the invention extends also to similar systems with more restricted coverage (for example of one or more continents).

Whilst the foregoing embodiments describe duplex communications systems, it will be clear that the invention is equally applicable to simplex (one way) transmission systems such as point-to-multipoint or broadcast systems.

Equally, whilst the preceding embodiments described direct transmission systems, it will be clear that the invention is applicable to store-and-forward communications systems in which one party transmits a message for storage and subsequent later delivery or transmission to the other party.

One example of such a store-and-forward system is e-mail, for example of the type provided by Compuserve (TM) or MCI (TM). Another example is the Internet, which, as is well known, consists of a number of host computer sites interconnected by a backbone of high speed packet transmission links, and accessible for file transfer from most points in the world via public telecommunications or other networks.

In an embodiment of this type, a central database station 15 need not distribute keys to both terminals at the same time; instead, distribution of the partial key to the transmitting terminal may take place at the time of transmission of a file of data for storage in encrypted form, and distribution of a partial key to the receiving terminal may take place substantially

later; for example, at the next occasion when the receiving terminal is connected to the network and/or the next occasion when the receiving terminal wishes to download the file from intermediate storage in a host computer.

Naturally, it will be understood that whilst the above embodiments discuss voice transmission, the invention is applicable to the encryption of data of any kind and particularly, but not exclusively, to image data, video data, text files or the like.

It will be understood that the geographical locations of the various components of the invention are not important, and that different parts of the system of the above embodiments may be provided in different national jurisdictions. For the avoidance of doubt, the present invention extends to any part or component of telecommunications apparatus or systems which contributes to the inventive concept.

The foregoing, and all other variants, embodiments, modifications or improvements to the invention are intended to be comprised within the present invention.

CLAIMS:

1. A method of distributing, through a communications network, enciphering key data for secure communication via said network between first and second terminals (2a,2b) each storing corresponding first and second terminal keys (K_a,K_b) comprising:

storing said first and second terminal keys (K_a,K_b) remotely to said terminals (2a,2b);

generating first and second corresponding partial keys (K_{pa},K_{pb}) each comprising a corresponding masking function of a corresponding one of said terminal keys (K_a,K_b); and

dispatching the first partial key (K_{pa}) towards the second terminal (2b), and vice-versa.

2. A method according to claim 1, further comprising providing a number (RAND), and in which each masking function is a joint function of said number and a corresponding said terminal key.

3. A method according to claim 2, in which the first and second functions comprise an Exclusive-OR.

4. A method according to claim 1, in which the first and second functions are the same.

5. A method according to any preceding claim, further comprising receiving a request signal requesting enciphering.

6. A method according to claim 5 when appended to claim 2, in which said step of providing comprises providing a new said number (RAND) in response to said

request signal.

7. A method according to claim 2 or any of claims 3 to 6 when appended thereto, in which said step of providing a number comprises pseudo randomly generating said number.

8. A method according to any preceding claim, further comprising a step of enciphering at least one of said first and second partial keys (K_{pa}, K_{pb}) prior to said step of dispatching.

9. A method according to claim 8 in which each of said first and second keys is enciphered with a different cipher.

10. A method according to claim 9 in which each of said first and second keys is enciphered with a common enciphering algorithm using said first and second keys as ciphering keys.

11. A method according to any preceding claim, further comprising a step of authenticating at least one said terminal (2a,2b) through a signalling dialogue, prior to said step of dispatching.

12. A method according to any preceding claim, further comprising separating access to said partial keys and functions at the location (15) where they are generated.

13. A method of communication between two terminals (2a,2b) through a communications network comprising:

distributing enciphering key data to said first

and second terminals via said network from a remote location;

using said enciphering key data to derive an enciphering key (K_{ab}) at each of said terminals (2a,2b);

enciphering data for transmission at a first said terminal (2a);

transmitting said enciphered data through said communications network;

receiving said enciphered data at the second terminal (2b); and

deciphering said enciphered data.

14. A method according to claim 13 in which at least one of the terminals (2a,2b) is mobile.

15. A method according to claim 13 or claim 14 in which the communications path to at least one of the terminals includes an air interface.

16. A method according to claim 15 in which said air interface includes a repeater satellite (4a,4b).

17. A method according to claim 15 in which said air interface includes a terrestrial radio link.

18. A method according to any of claims 15 to 17 in which a further stage of encryption is provided over the or each said air interface.

19. A method according to claim 13, further comprising a step of storing said data.

20. A method according to claim 19 in which said communications network comprises at least one computer

via which data may be transferred in the form of message files.

21. A method of secure communication between two terminals (2a,2b) comprising providing each terminal with a terminal key (K_a,K_b); sending each terminal data relating to the other is terminal key; and carrying encrypted traffic from a first said terminal (2a) to a second (2b) in a cipher (K_{ab}) depending on both said terminal keys (K_a, K_b).

22. A method according to claim 21, further comprising providing storage means (15) separate from said terminals (2a,2b) storing data relating to said terminal keys, and in which the terminal keys are sent to each terminal from the storage means (15).

23. A method according to claim 22 in which said keys (K_a,K_b) are sent in encoded form (K_{pa},K_{pb}).

24. A method according to claim 23 comprising generating each said encoded form (K_{pa},K_{pb}) as the product of the corresponding terminal key and a predetermined number (RAND).

25. A method of secure communication between two mobile terminals (2a,2b) in a satellite communications system, comprising enciphering data at a first said terminal (2a), carrying said data in enciphered form on the entire path through said network to said second terminal (2b), and deciphering said data at said second terminal (2b).

26. A method of secure communication between two mobile terminals (2a,2b) each of which is connected

via an air interface to a terrestrial transceiver station (6a,6b), comprising applying first encryption between each terminal (2a,2b) and the terrestrial transceiver station (6a,6b), said first encryption being applied at said transceiver station (6), and applying second encryption over the whole path through the network between said first and second terminals (2a,2b).

27. Apparatus (15) for storing enciphering key data for enabling secure communications via a network between first and second terminals (2a,2b) each storing corresponding first and second terminal keys (K_a,K_b), said apparatus comprising:

a store (54) containing said terminal keys (K_a,K_b,...); and

means (56) for communicating with said network;

means (58) for sending a first said terminal key (K_a) to a second said terminal (2_b) and a second said terminal key (K_b) to a first said terminal (K_a), to enable end-to-end enciphered communications between said terminals (2a,2b).

28. Apparatus (15) according to claim 27 further comprising means (58) for masking each said terminal key (K_a,K_b...) prior to sending thereof.

29. Signal routing apparatus (6a,6b) for routing signals from a first terminal (2a) to a second terminal (2b) via a communications network, said routing apparatus comprising:

means (72) for receiving a signal indicating a requesting for end-to-end encrypted communications between said first and second terminals (2a,2b);

means (74) for indicating said request to a

further station (15) holding encryption key data;

means (76) for receiving said enciphering data from said further station (15); and

means for forwarding said enciphering data to a said mobile terminal (2a).

30. A first terminal (2a) for communicating, via a communications network, with a second terminal (2b), said first terminal comprising:

a store (35b) containing a terminal key (K_a) for said first terminal;

a receiver port (31,32) coupled to said communications network;

a processor device (35a) coupled to said receiver port to receive therefrom data (K_{pb}) relating to a terminal key (K_b) held at said second terminal (2b);

a key generator (35a) arranged to calculate from said data (K_{pb}) and said terminal key of (K_a) said first terminal an enciphering key ($K_{a,b}$) depending on both said terminal keys; and

enciphering/deciphering apparatus (37) arranged to encipher and/or decipher data transmitted from and/or received at said terminal (2a) in accordance with said enciphering key ($K_{a,b}$).

31. Apparatus according to claim 30 in which said store (35b) and said processor device (35a) are provided within a secure device (35) which cannot be read from an external device.

32. Apparatus according to claim 31, in which said secure device (35) comprises a removable and insertable module (35).

33. Apparatus according to any of claims 30 to

32 which further comprises air interface components (31,32) for communicating via an air interface with said network.

34. Apparatus according to claim 34, in which said air interface components (31,32) are for communicating with a satellite (4a,4b).

35. Secure data storage apparatus (35) comprising a store (35b) for storing terminal key data (K_a) and a processor (35a) for receiving further terminal key data (K_{pb}) and for combing said further terminal key data (K_{pb}) with said stored terminal key data (K_a) and for generating, responsive thereto, a combined encryption key (K_{ab}).

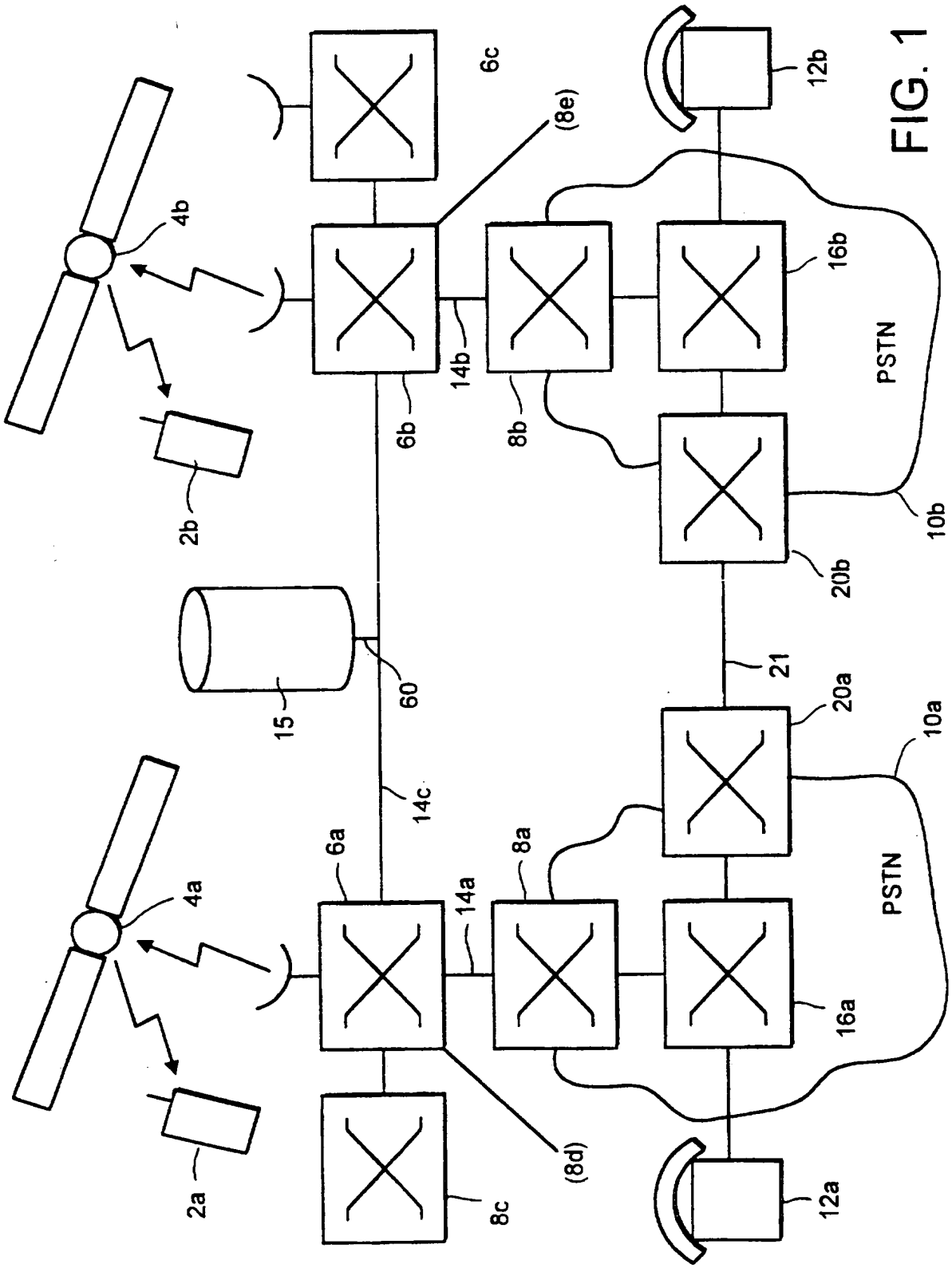
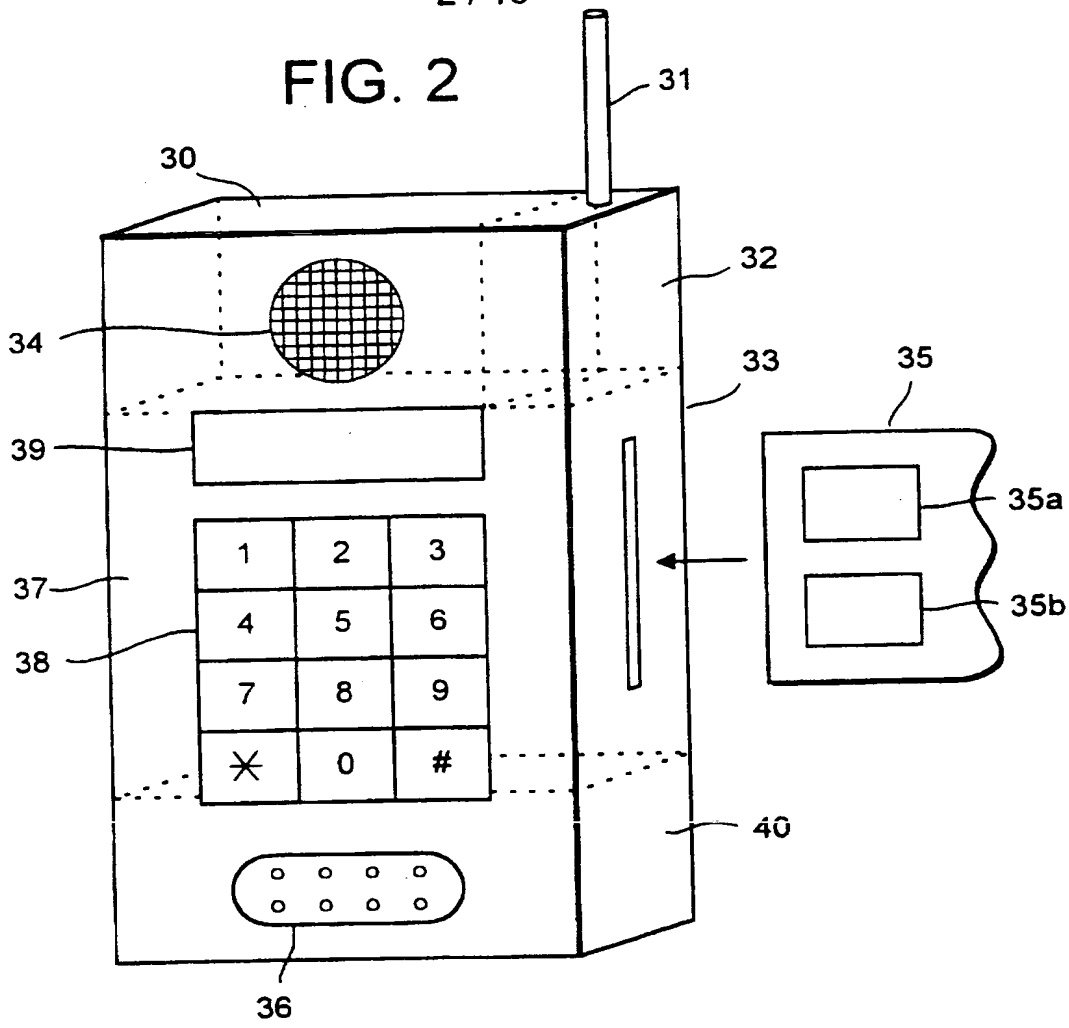

6c
(8e)
12b
4b
16b
14b
6b
8b
PSTN
2b
10b
20b
21
60
15
20a
10a
14c
6a
8a
4a
14a
PSTN
16a
(8d)
2a
8c
12a

FIG. 1

FIG. 2


31
30
32
34
33
35
39
35a
1
2
3
37
4
5
6
35b
38
7
8
9
*
0
#
40
36

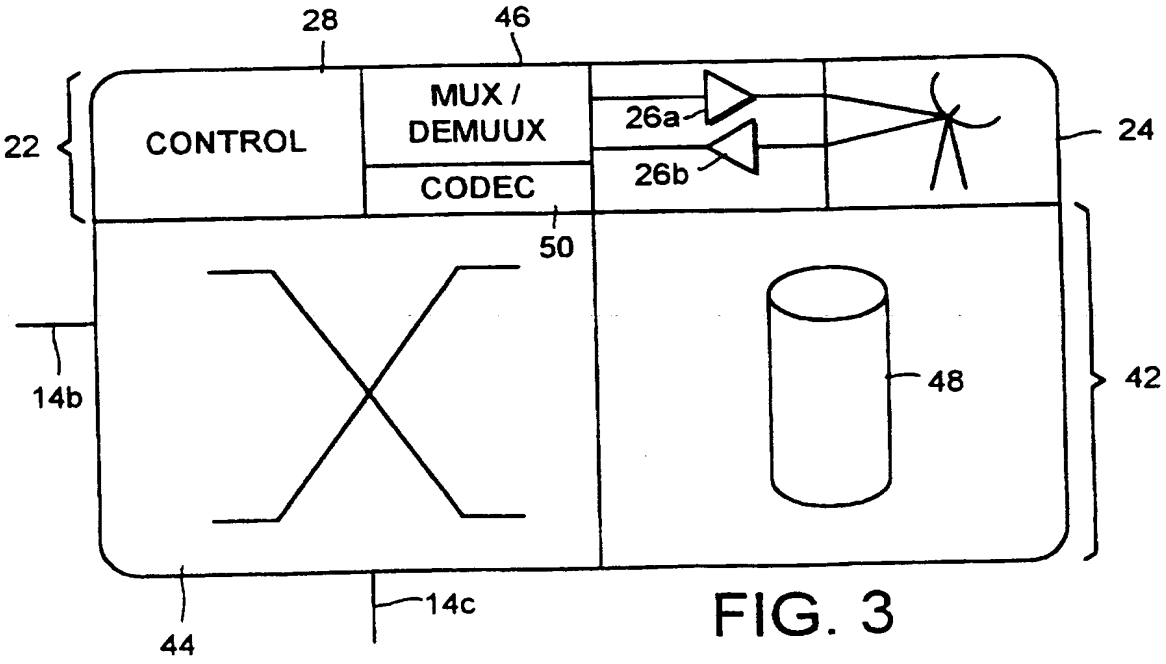

28
46
22
CONTROL
MUX / DEMUUX
CODEC
26a
26b
24
50
14b
48
42
44
14c

FIG. 3

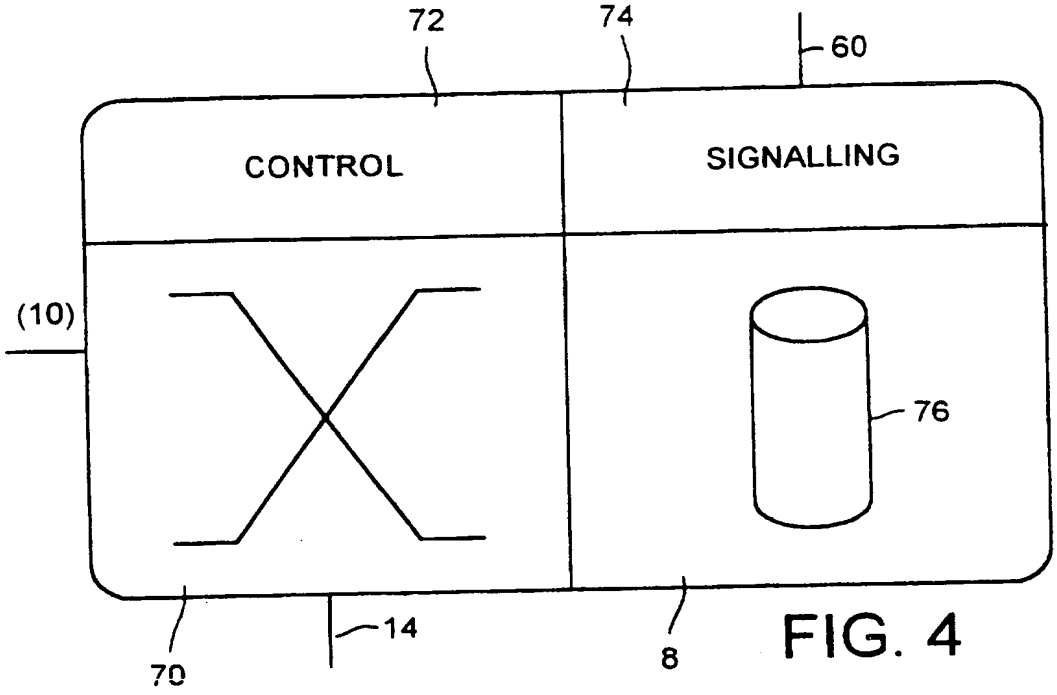

72
74
60
CONTROL
SIGNALLING
(10)
76
70
14
8

FIG. 4

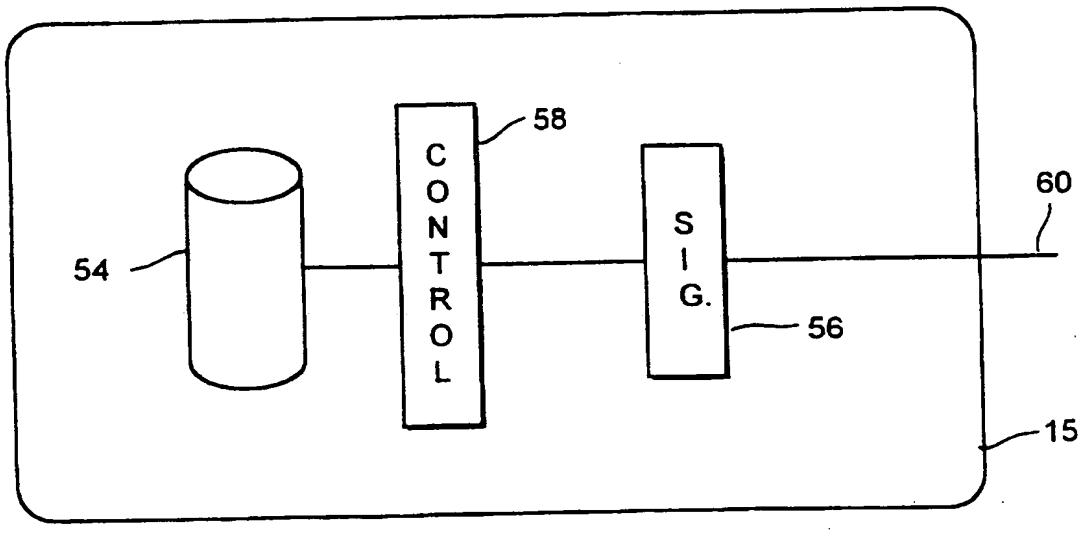

58
CONTROL
SIG.
60
54
56
15

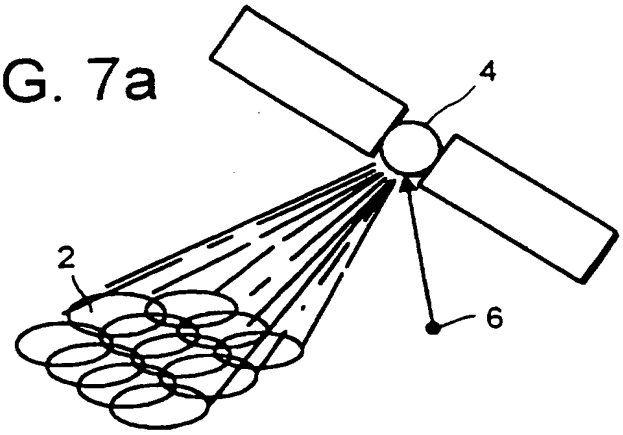
FIG. 5

54

ID #	KEY Ki	STATUS	POSITION	ACTIV NODE	AVAIL ?	HOME
00001	K_A	LOCAL	46°, 35°	6a	Y	8a
00002	K_B	GLOBAL	71°, 27°	6b	Y	8b

FIG. 6

FIG. 7a



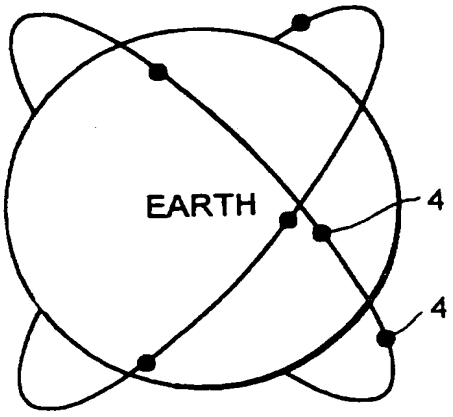


FIG. 7b

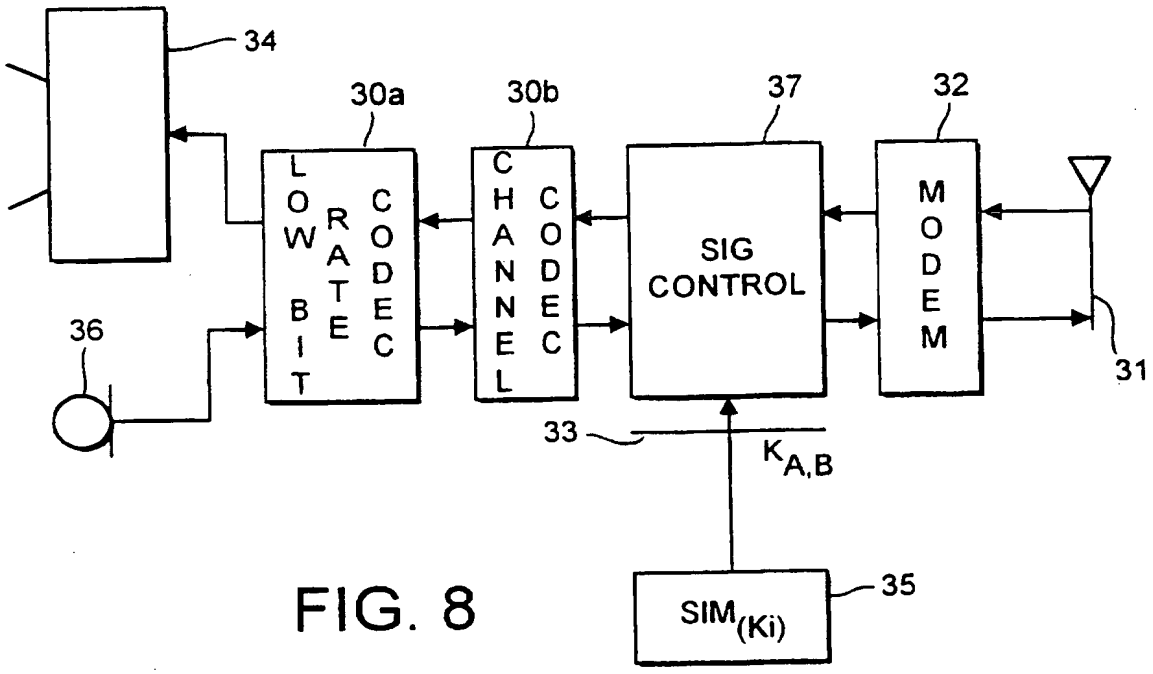

34
30a
30b
37
32
LOW BIT RATE CODEC
CHANNEL CODEC
SIG CONTROL
MODEM
36
31
33
$K_{A,B}$
$SIM_{(Ki)}$
35

FIG. 8

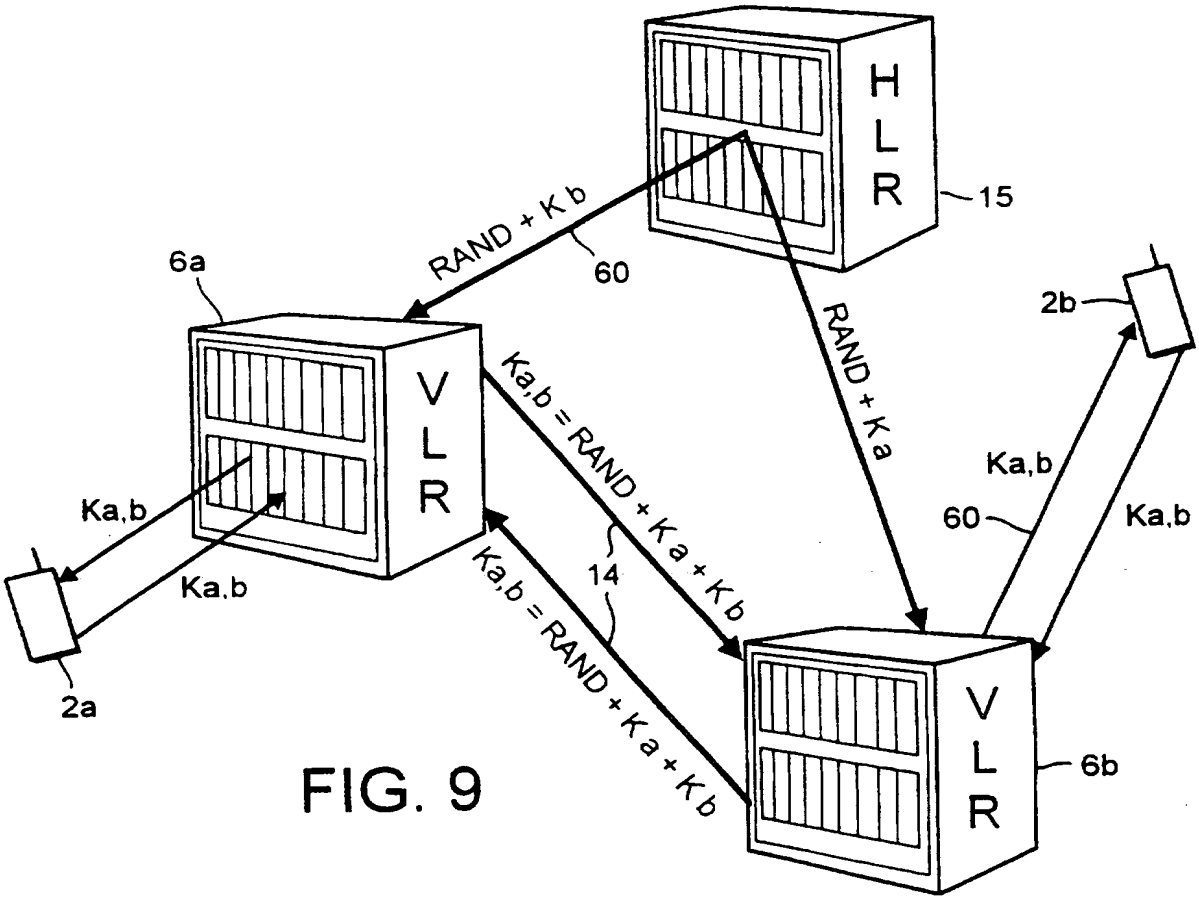

HLR
15
RAND + K b
60
6a
VLR
Ka,b = RAND + Ka + Kb
RAND + Ka
2b
Ka,b
60
Ka,b
Ka,b
Ka,b
14
Ka,b = RAND + Ka + Kb
2a
VLR
6b

FIG. 9

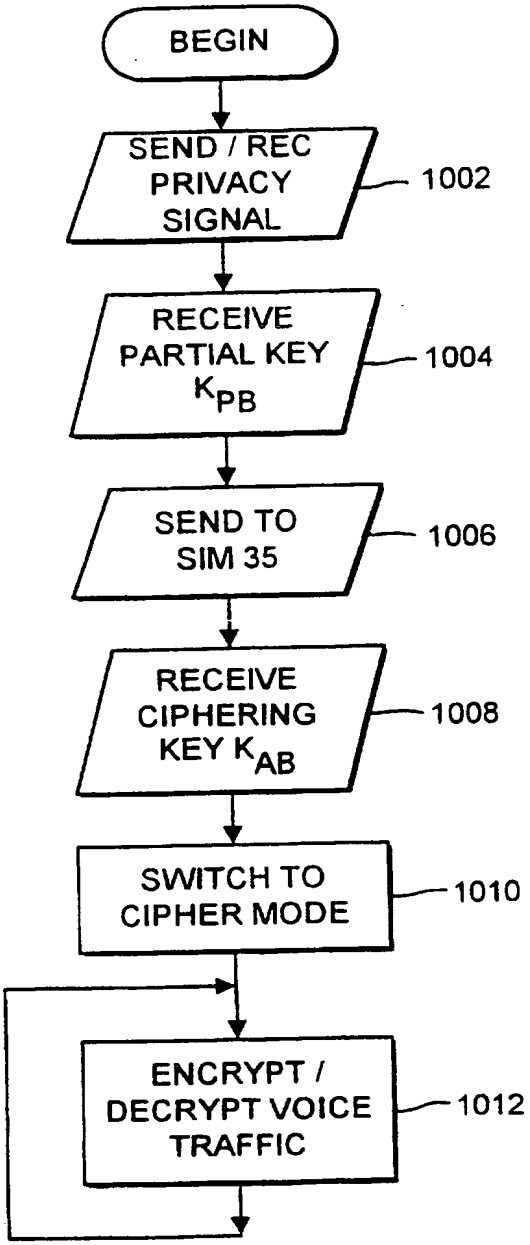


FIG. 10a

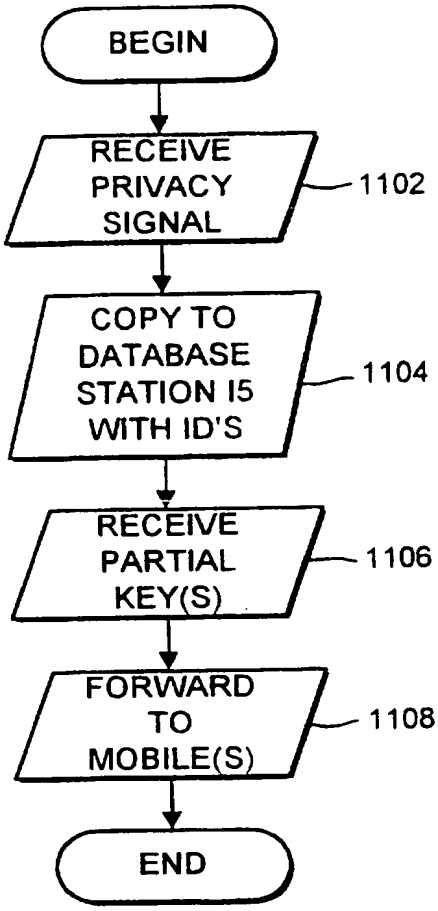


FIG. 10b

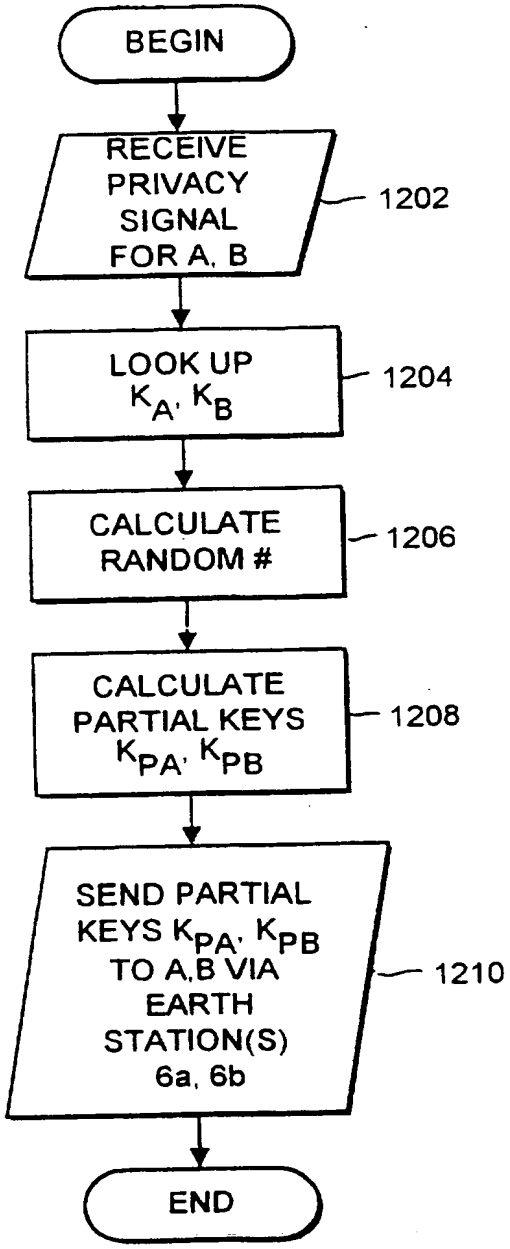


FIG. 10c

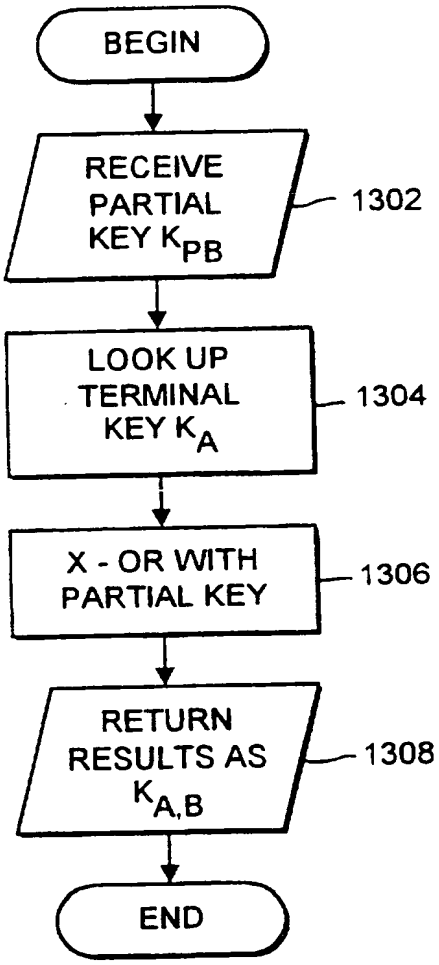


FIG. 10d

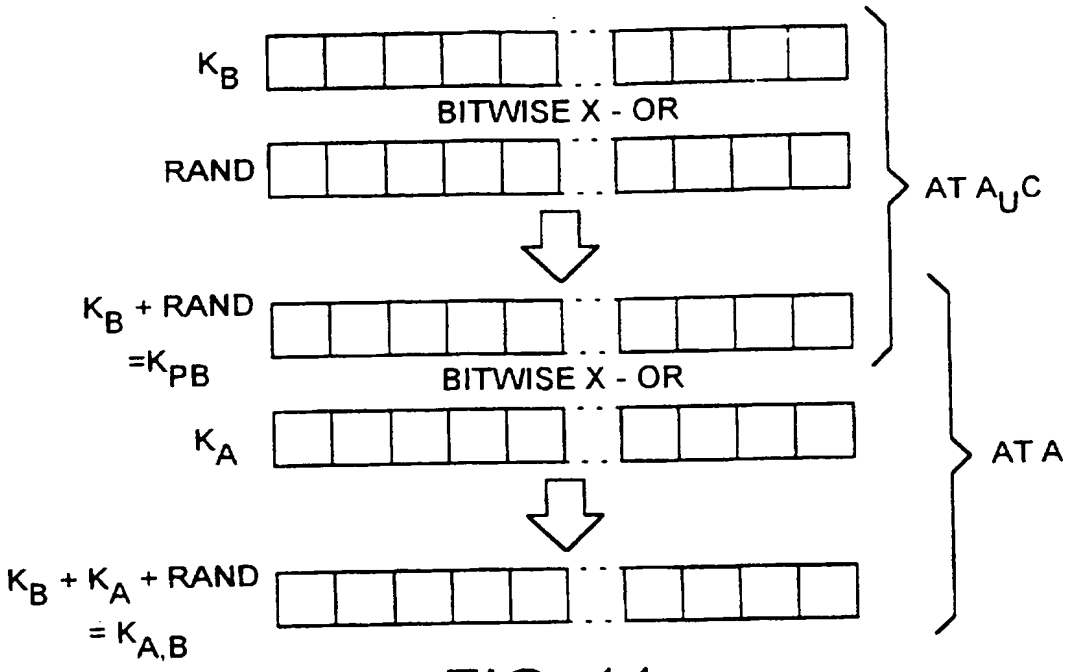


FIG. 11a

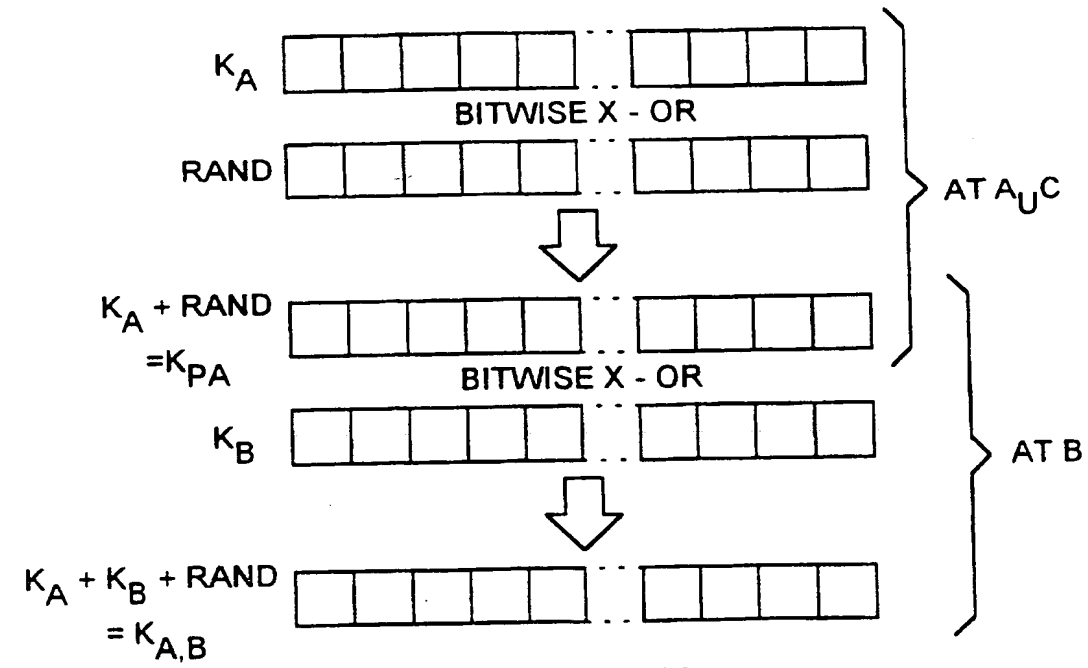


FIG. 11b

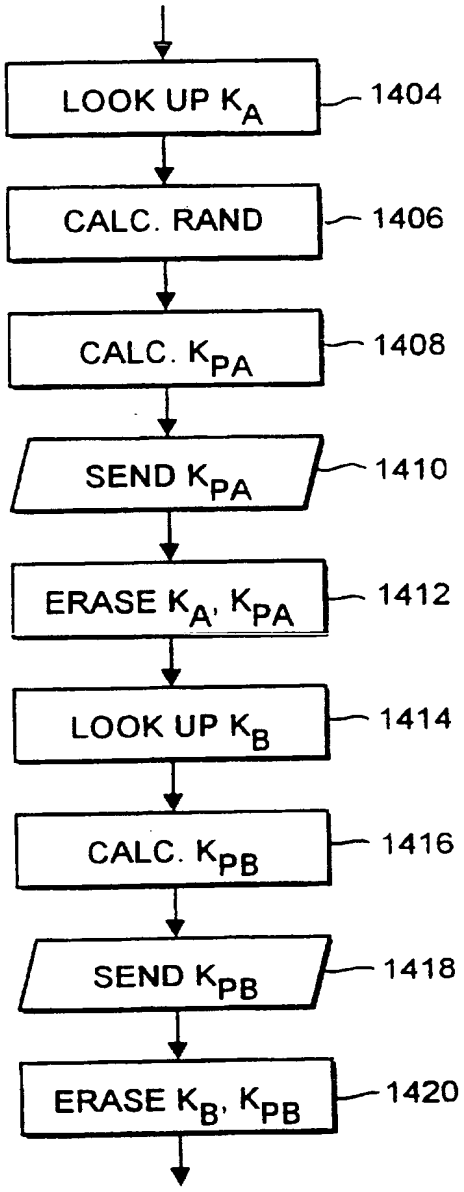


FIG. 12

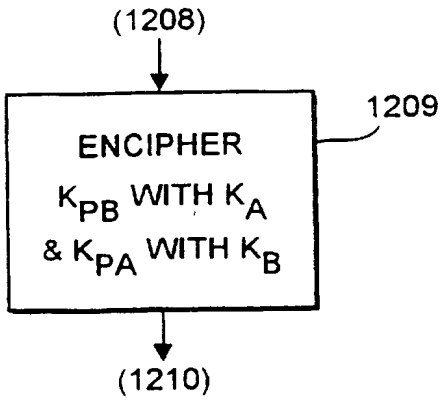


FIG. 13a

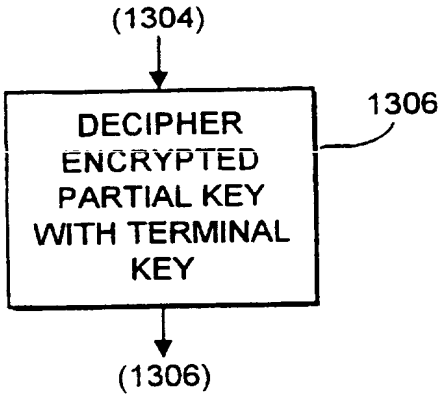


FIG. 13b

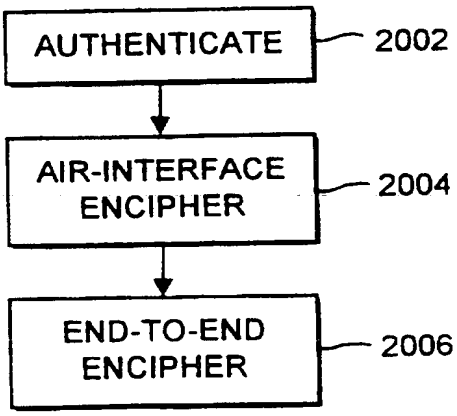


FIG. 14

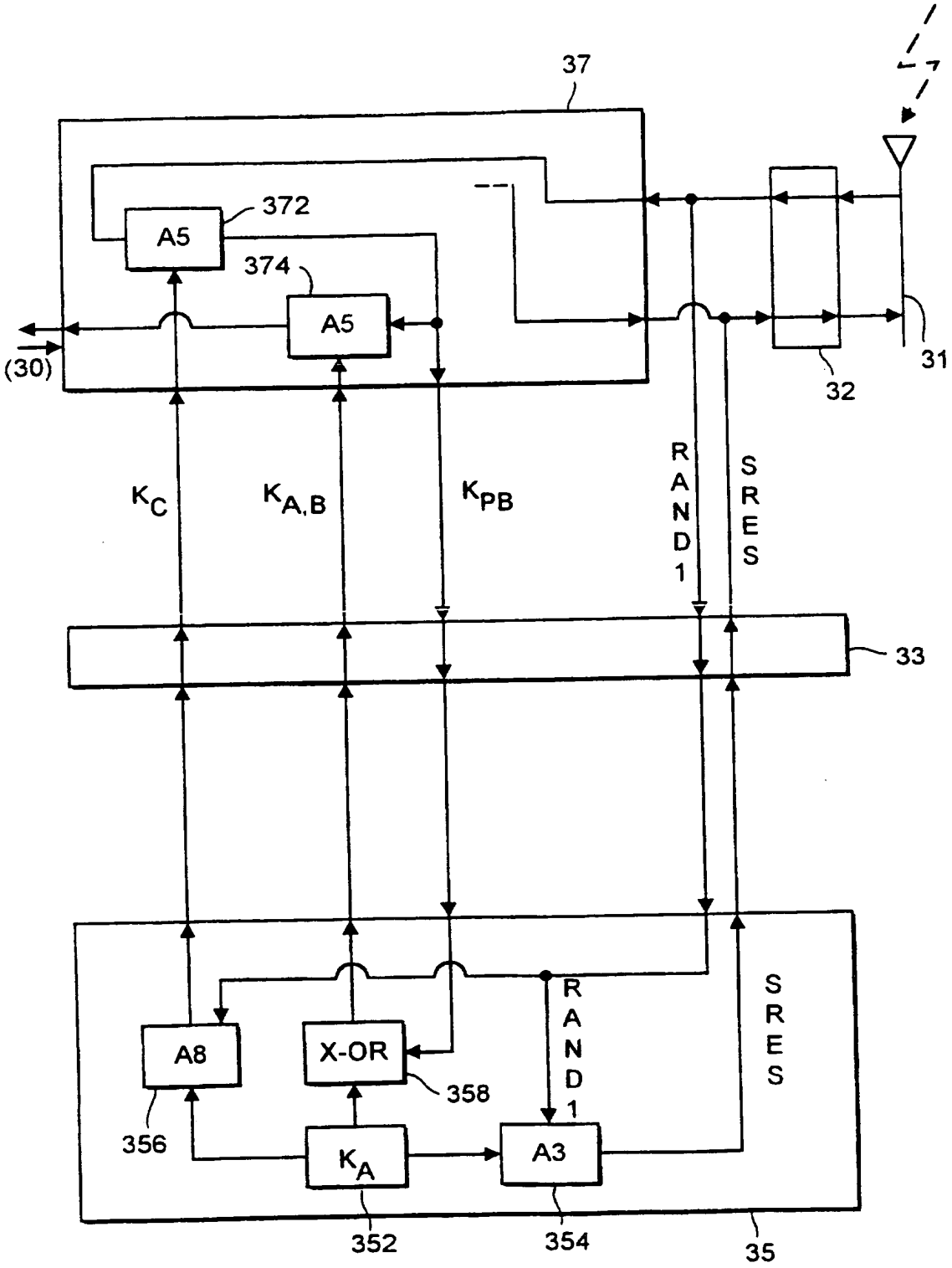

37
372
A5
374
A5
(30)
32
31
K_C
$K_{A,B}$
K_{PB}
RAND 1
SRES
33
A8
X-OR
358
356
K_A
A3
RAND 1
SRES
352
354
35

FIG. 15a

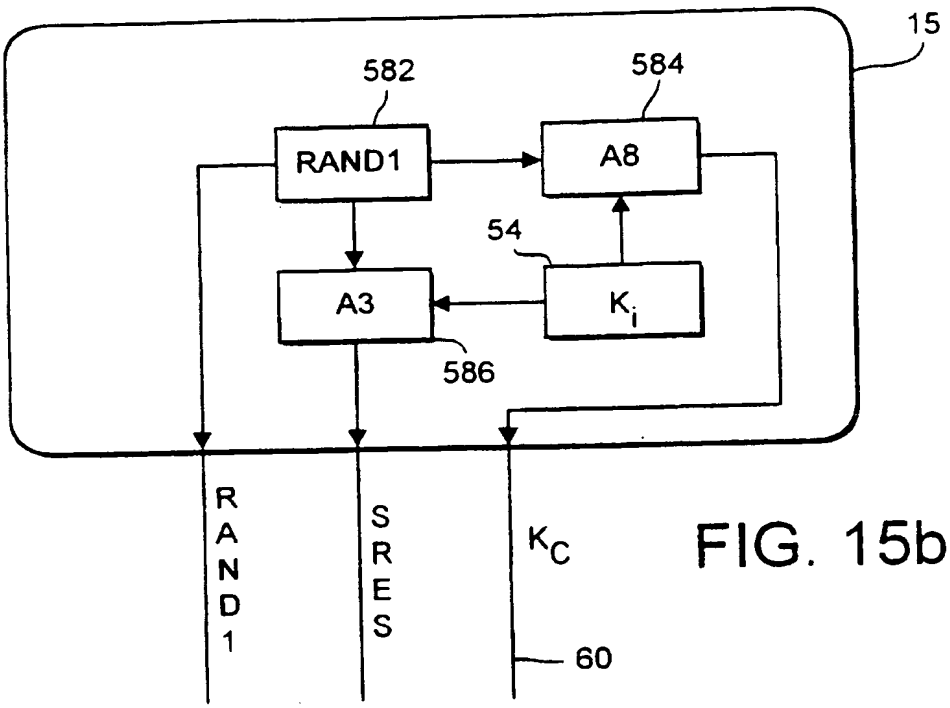


FIG. 15b

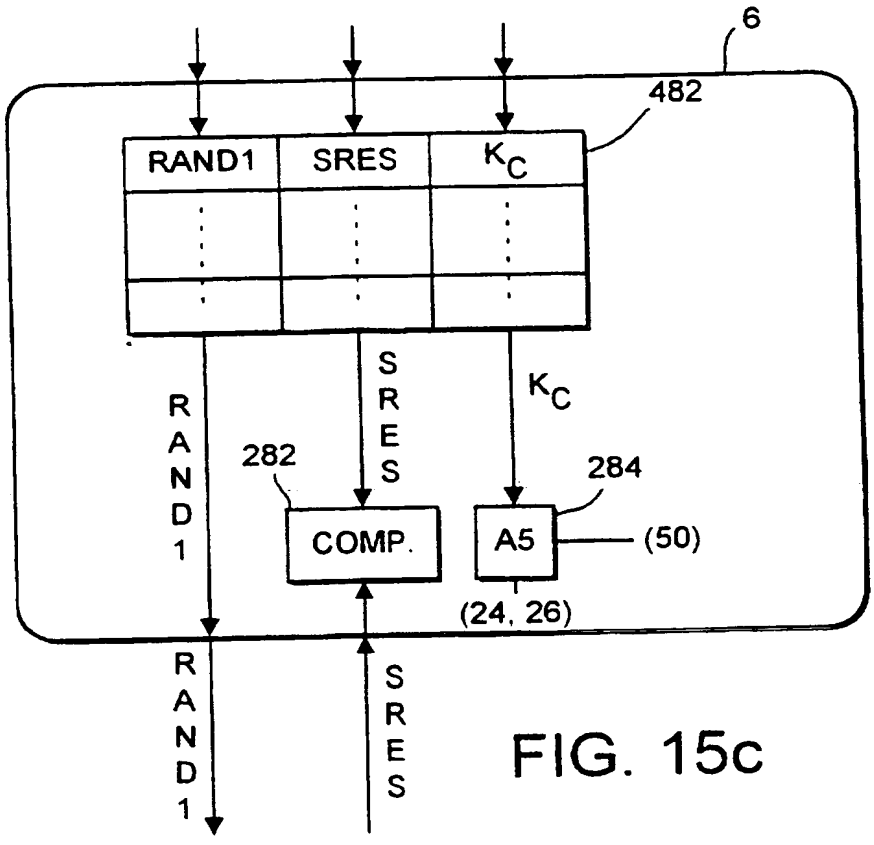


FIG. 15c

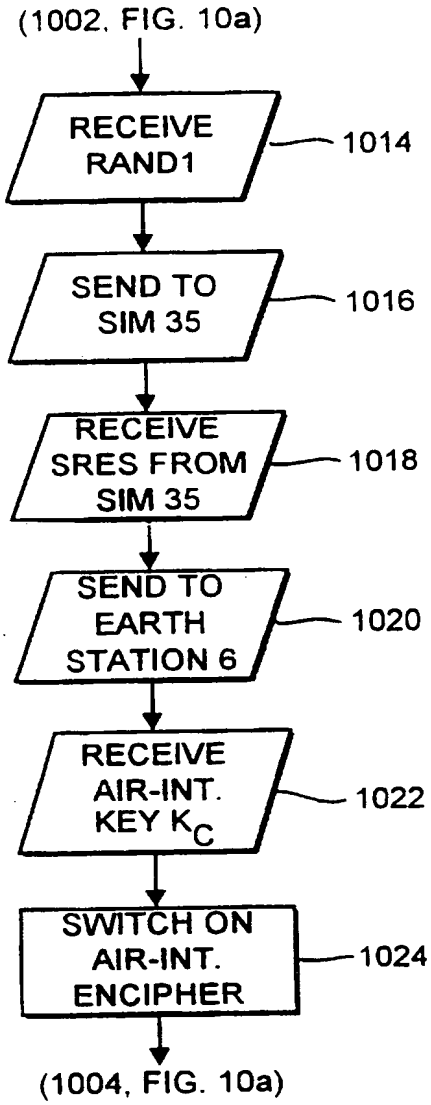


FIG. 16a

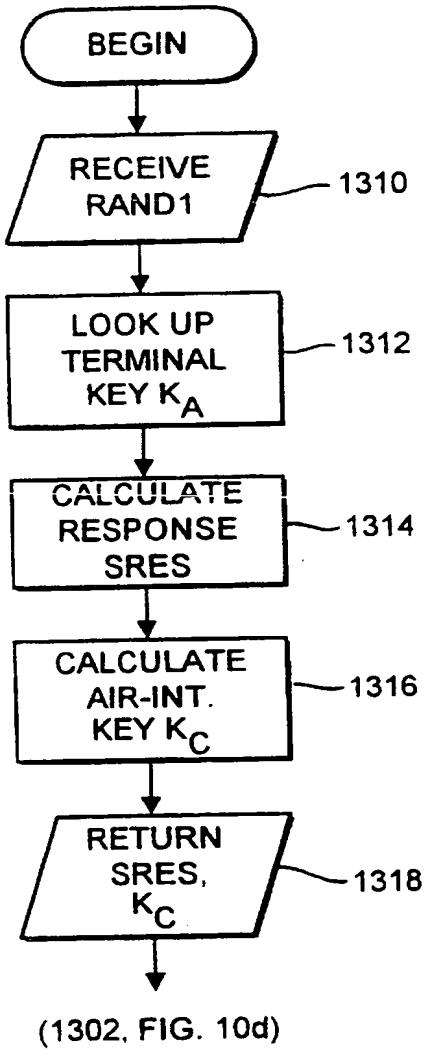


FIG. 16d

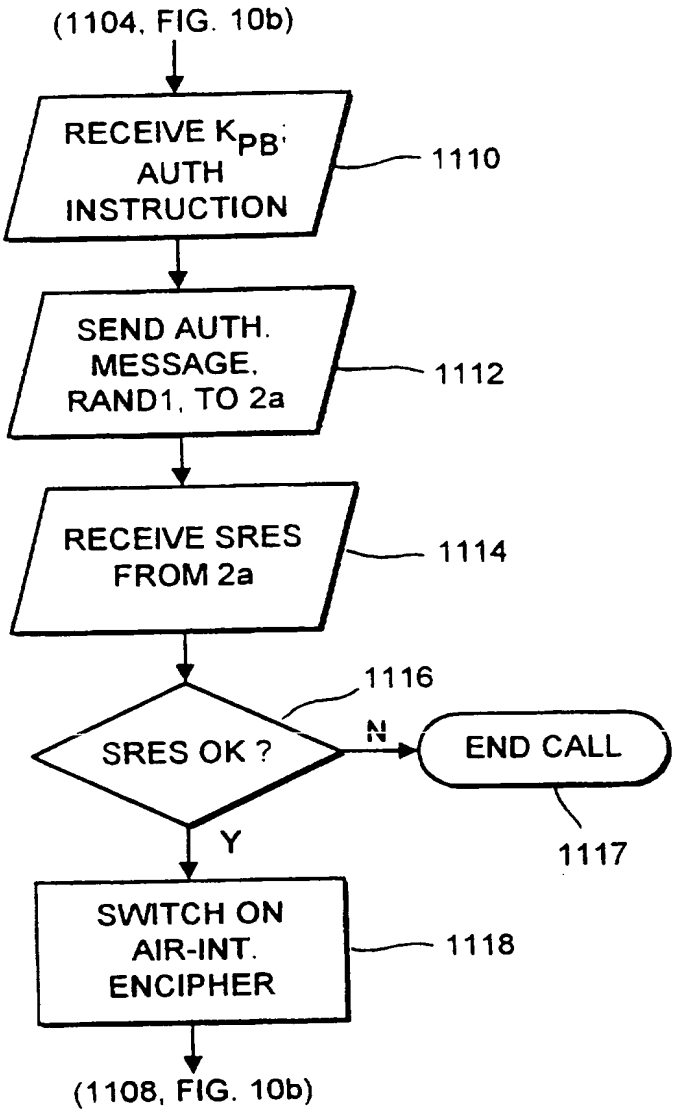


FIG. 16b

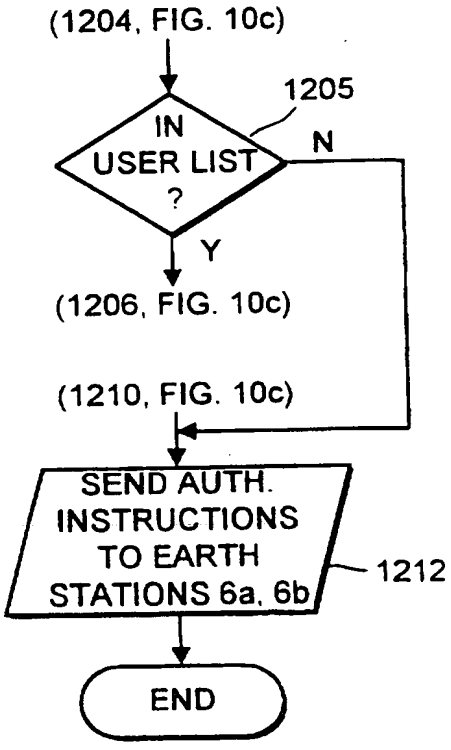


FIG. 16c

INTERNATIONAL SEARCH REPORT

Interna ..al Application No
PCT/GB 97/01407

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 688 140 A (INFORMATIKZENTRUM DER SPARKASS) 20 December 1995 see column 2, line 53 - line 58 see column 3, line 24 - line 30 see column 3, line 53 - column 4, line 4 see column 5, line 10 - last line ---	1,2,5, 13-15
X	CAMPANINI ET AL. : "PRIVACY, SECURITY AND USER IDENTIFICATION IN NEW GENERATION RADIOMOBILE SYSTEMS" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS, 30 June 1987, VENICE (IT), pages 152-164, XP002040784 see page 159, line 9 - page 160, line 21 --- -/--	1,5, 13-15, 17,29

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 September 1997	29. 09. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna...al Application No
PCT/GB 97/01407

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DIFFIE ET AL.: "MULTIUSER CRYPTOGRAPHIC TECHNIQUES" AFIPS CONFERENCE PROCEEDINGS OF NATIONAL COMPUTER CONFERENCE, vol. 45, June 1976, pages 109-112, XP002040785 see page 110, left-hand column, line 19 - line 36 ---	1,13
X	EP 0 365 885 A (MOTOROLA) 2 May 1990 see abstract see column 7, last paragraph ---	25
A	FR 2 608 338 A (ELECTRONIQUE SERGE DASSAULT) 17 June 1988 see page 3, line 21 - line 33 see page 4, line 30 - line 34 see page 9, line 18 - line 32 ---	35
A	AREND VAN DER P C J: "SECURITY ASPECTS AND THE IMPLEMENTATION IN THE GSM-SYSTEM" PROCEEDINGS OF DIGITAL CELLULAR RADIO CONFERENCE, 12 October 1988, pages 4A/1-4A/07, XP000618482 cited in the application see page 4A2, last paragraph - page 4A3, line 20 -----	1,13

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna .ial Application No
PCT/GB 97/01407

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0688140 A	20-12-95	NONE	
EP 365885 A	02-05-90	AT 127974 T	15-09-95
		AU 628081 B	10-09-92
		AU 4169389 A	03-05-90
		CA 1338020 A	30-01-96
		CN 1042278 A,B	16-05-90
		DE 68924234 D	19-10-95
		DE 68924234 T	02-05-96
		EG 19299 A	29-06-95
		ES 2076945 T	16-11-95
		HK 113996 A	05-07-96
		HR 940222 A	30-04-96
		JP 2179035 A	12-07-90
		KR 9707988 B	19-05-97
		NO 177480 B	12-06-95
		OA 9055 A	31-03-91
		PL 167049 B	31-07-95
		PT 92102 B	31-05-96
		TR 25340 A	01-03-93
		US 5410728 A	25-04-95
FR 2608338 A	17-06-88	NONE	

第 7 部門第 3 区分　　全 17 頁

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号

特表平11－510668

(43)公表日　平成11年(1999) 9月14日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ｄ
Ｈ０４Ｂ　7/212				６０１Ａ
Ｈ０４Ｑ　7/38				６０１Ｅ
		Ｈ０４Ｂ	7/26	１０９Ｒ
			7/15	Ｃ

審査請求　未請求　　予備審査請求　未請求(全 50 頁)

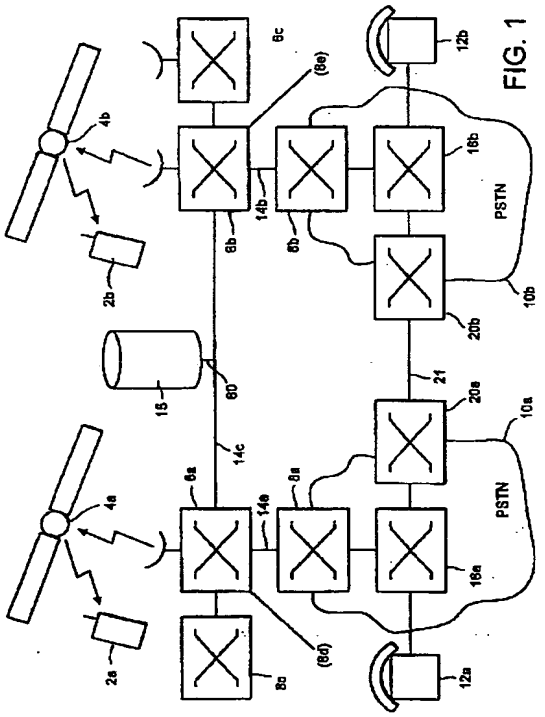
(21)出願番号　特願平9－541825
(86) (22)出願日　平成９年(1997) ５月23日
(85)翻訳文提出日　平成10年(1998) ２月２日
(86)国際出願番号　ＰＣＴ／ＧＢ９７／０１４０７
(87)国際公開番号　ＷＯ９７／４５９８１
(87)国際公開日　平成９年(1997)12月４日
(31)優先権主張番号　９６１１４１１．１
(32)優先日　1996年５月31日
(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　アイシーオー　サーヴィシーズ　リミテッド
イギリス国　Ｗ６　９ＢＮ　ロンドン　クィーン　キャロライン　ストリート　１
(72)発明者　ジョンストン，トーマス　フランシス
イギリス国　Ｗ２　６ＤＧ　ロンドン　クリーヴランド　スクエア　22エー
(74)代理人　弁理士　志賀　正武　（外１名）

最終頁に続く

(54)【発明の名称】　セキュリティ通信

(57)【要約】
通信回線網を介したセキュリティ通信セッション用の第１と第２の端末機鍵（Ka，Kb）に対応する暗号化鍵を、第１と第２の端末機（２ａ、２ｂ）の間で前記回線網を経て配分する方法であって、前記第１と第２の端末機鍵（Ka，Kb）を前記端末機（２ａ、２ｂ）に遠隔記憶するステップと、数字（ＲＡＮＤ）を供給するステップと、それぞれが前記数字（ＲＡＮＤ）の対応する関数と、前記端末機鍵（Ka，Kb）の対応する関数とからなる前記第１と第２の対応する部分鍵（Kpa，Kpb）を生成するステップと、第１部分鍵（Kpa）を第２端末機（２ｂ）の方向に、またその逆に発信（ディスパッチ）するステップと、からなることを特徴とする方法である。



【特許請求の範囲】

１．　通信回線網を経たセキュリティ通信用の暗号化鍵データを、それぞれが対応する第１と第２の端末機鍵（Ka，Kb）を記憶している第１と第２の端末機（２ａ、２ｂ）の間で前記回線網を介して配分する方法において、

前記第１と第２の端末機鍵（Ka，Kb）を前記端末機（２ａ、２ｂ）に遠隔記憶するステップと、

それぞれが前記端末機鍵（Ka，Kb）のうちの対応する一方の対応するマスキング機能をなす第１と第２の対応する部分鍵（Kpa，Kpb）を生成するステップと、

第１部分鍵（Kpa）を第２端末機（２ｂ）の方向に、またその逆に発信（ディスパッチ）するステップと、からなることを特徴とする方法。

２．　数字（ＲＡＮＤ）を供給するステップを更に含み、マスキング関数は前記数字と、対応する前記端末機鍵との結合関数であることを特徴とする請求項１記載の方法。

３．　第１と第２の関数は排他的ＯＲ演算からなることを特徴とする請求項２記載の方法。

４．　第１と第２の関数が同一であることを特徴とする請求項１記載の方法。

５．　暗号化を要求する要求信号を受信するステップを更に含むことを特徴とする請求項１から請求項４のいずれかに記載の方法。

６．　前記数字を供給するステップが前記要求信号に応答して新たな前記数字（ＲＡＮＤ）を供給するステップからなることを特徴とする請求の範囲第２項に追加した請求項５記載の方法。

７．　前記数字を供給するステップが疑似乱数的に前記数字を生成するステップからなることを特徴とする請求項２、またはこれに追加した請求項３から請求項６のいずれかに記載の方法。

８．　前記発信ステップの前に前記第１と第２の部分鍵（Kpa，Kpb）の少なくとも一方を暗号化するステップを更に含むことを特徴とする請求項１から請求項７のいずれかに記載の方法。

９．　前記第１と第２の鍵のそれぞれが異なる暗号で暗号化されることを特徴とする請求項８記載の方法。

１０．　前記第１と第２の鍵のそれぞれが前記第１と第２の鍵を暗号化鍵として用いた共通の暗号化アルゴリズムで暗号化されることを特徴とする請求項９記載の方法。

１１．　前記発信ステップの前に、信号通信の対話を介して前記端末機（２ａ、２ｂ）の少なくとも一方を認証するステップを更に含むことを特徴とする請求項１から請求項１０のいずれかに記載の方法。

１２．　前記部分鍵と関数へのアクセスをそれらが生成されたロケーション（１５）で分離するステップを更に含むことを特徴とする請求項１から請求項１１のいずれかに記載の方法。

１３．　通信回線網を経て２つの端末機（２ａ、２ｂ）間で通信する方法において、

遠隔位置から前記回線網を介して第１と第２の端末機に暗号化鍵データを配分するステップと、

前記暗号化鍵データを用いて前記端末機（２ａ、２ｂ）のそれぞれで暗号化鍵（Kab）を導出するステップと、

前記第１端末機（２ａ）で前記暗号化されたデータを送信するステップと、

前記通信回線網を介して前記暗号化されたデータを送信するステップと、

前記第２端末機（２ｂ）で前記暗号化されたデータを受信するステップと、

前記暗号化されたデータを暗号解読するステップと、からなることを特徴とする方法。

１４．　端末機（２ａ、２ｂ）の少なくとも一方が移動体であることを特徴とする請求項１３記載の方法。

１５．　少なくとも１つの端末機への通信経路がエアインターフェースを含むことを特徴とする請求項１３、または請求項１４に記載の方法。

１６．　前記エアインターフェースが中継衛星（４ａ、４ｂ）を含むことを特徴とする請求項１５記載の方法。

１７．　前記エアインターフェースが地上無線リンクを含むことを特徴とする請求項１５記載の方法。

１８．　前記エアインターフェース、またはその各々に暗号化段を更に備えたことを特徴とする請求項１５から請求項１７のいずれかに記載の方法。

１９．　前記データを記憶するステップを更に含むことを特徴とする請求項１３記載の方法。

２０．　前記通信回線網が、それを介してデータをメッセージ・ファイルの形式で伝送できる少なくとも１つのコンピュータを備えたとを特徴とする請求項１９記載の方法。

２１．　２つの端末機（２ａ、２ｂ）の間のセキュリティ通信の方法において、それぞれの端末機（２ａ、２ｂ）に端末機鍵（Ka，Kb）を供給するステップと、それぞれの端末機に他の端末機に関するデータである端末機鍵を送信するステップと、前記双方の端末機鍵（Ka，Kb）に従って、第１の前記端末機（２ａ）から第２の端末機（２ｂ）に暗号（Kab）で暗号化された交信を搬送するステップとからなることを特徴とする方法。

２２．　前記端末機鍵に関するデータを記憶する前記端末機（２ａ、２ｂ）から離れた記憶手段（１５）をさらに備えるとともに、端末機鍵が記憶手段（１５）から各端末機に送信されることを特徴とする請求項２１記載の方法。

２３．　前記鍵（Ka，Kb）がコード化された形式（Kpa，Kpb）で送信されることを特徴とする請求項２２記載の方法。

２４．　前記各々のコード化された形式（Kpa，Kpb）を対応する端末機鍵と所定数（ＲＡＮＤ）の積として生成することを特徴とする請求項２３記載の方法。

２５．　衛星通信システムで２つの移動体端末機（２ａ、２ｂ）間のセキュリティ通信を行う方法において、前記第１端末機（２ａ）でデータを暗号化するステップと、前記データを暗号化された形式で前記回線網の全経路で前記第２端末機（２ｂ）へと搬送するステップと、前記データを前記第２端末機（２ｂ）で暗号解読するステップと、からなることを特徴とする方法。

２６．　それぞれがエアインターフェースで地上トランシーバ局（６ａ、６ｂ）に接続さている２つの移動体端末機（２ａ、２ｂ）間でセキュリティ通信を行う方法において、各端末機（２ａ、２ｂ）と地上トランシーバ局（６ａ、６ｂ）との間で第１の暗号化を行い、前記第１の暗号化は前記トランシーバ局（６）にて行われるステップと、前記第１と第２の端末機（２ａ、２ｂ）の間の回線網を経た全経路に亘って第２の暗号化を行うステップと、からなることを特徴とする方法。

２７．　通信回線網を経て、それぞれが対応する第１と第２の端末機鍵（Ka，Kb）を記憶している第１と第２の端末機（２ａ、２ｂ）の間のセキュリティ通信を可能にするため暗号化鍵データを記憶する装置（１５）おいて、

前記端末機鍵（Ka，Kb，．．）を含む記憶装置（５４）と、

前記回線網と通信する手段（５６）と、

前記第１端末機鍵（Ka）を前記第２端末機（２ｂ）に送信し、前記第２端末機鍵（Kb）を前記第１端末機（Ka）に送信して、前記端末機（２ａ、２ｂ）間の端末機間暗号通信を可能にする手段（５８）とを備えて構成されたことを特徴とする装置。

２８．　前記端末機鍵（Ka，Kb，．．）を送信する前にそれぞれの端末機鍵をマスキングするための手段（５８）を更に備えたことを特徴とする請求項２７記載の装置（１５）。

２９．　通信回線網を経て第１端末機（２ａ）から第２端末機（２ｂ）への信号経路を指定する信号経路指定装置（６ａ、６ｂ）において、

前記第１と第２の端末機（２ａ、２ｂ）間の端末機間暗号通信の要求を示す信号を受信する手段（７２）と、

前記要求を暗号化鍵データを保存する別の局（１５）に示すための手段（７４）と、

前記別の局（１５）からの前記暗号化データを受信するための手段（７６）と、

前記暗号化データを前記移動体端末機（２ａ）に送るための手段と、

を備えて構成されたことを特徴とする装置。

３０．　通信回線網を介して第２端末機（２ｂ）と通信するための第１端末機（２ａ）において、

前記第１端末機用の端末機鍵（Ｋａ）を記憶している記憶装置（３５ｂ）と、

前記通信回線網と結合された受信機ポート（３１、３２）と、

前記受信機ポートと結合され、この受信機ポートから前記第２端末機（２ｂ）に保存された端末機鍵（Ｋｂ）に関するデータ（Ｋｐｂ）を受信するプロセッサ装置（３５ａ）と、

前記双方の端末機鍵に従って、前記第１端末機の前記データ（Ｋｐｂ）および前記端末機鍵（Ｋａ）から暗号化鍵（Ｋａ.ｂ）を計算するように構成された鍵発生器（３５ａ）と、

前記暗号化鍵（Ｋａ.ｂ）に従って前記端末機（２ａ）から送信され、および（または）そこで受信されたデータを暗号化および（または）暗号解読するように構成された暗号化／暗号解読装置（３７）と、

を備えて構成されたことを特徴とする第１端末機。

３１．　前記記憶装置（３５ｂ）と前記プロセッサ装置（３５ａ）とを外部装置からは読出すことができないセキュリティ装置（３５）内に備えたことを特徴とする請求項３０記載の装置。

３２．　前記セキュリティ装置（３５）が取り外し可能、かつ挿入可能なモジュール（３５）からなることを特徴とする請求項３１記載の装置。

３３．　エアインターフェースを介して前記回線網と通信するためのエアインターフェース部品（３１、３２）を更に備えたことを特徴とする請求項３０から請求項３２のいずれかに記載の装置。

３４．　前記エアインターフェース部品（３１、３２）が衛星（４ａ、４ｂ）との通信用の部品であることを特徴とする請求項３４記載の装置。

３５．　セキュリティ・データ記憶装置（３５）において、端末機鍵データ（Ｋａ）を記憶するための記憶装置（３５ｂ）と、更に別の端末機鍵データ（Ｋｐｂ）を受信し、かつ前記更に別の端末機鍵データ（Ｋｐｂ）と前記記憶された端末機鍵データ（Ｋａ）とを結合し、それに応答して結合された暗号化鍵（Ｋａｂ）を生成するプロセッサ（３５ａ）とを備えて構成されたことを特徴とするセキュリティ・データ記憶装置。

【発明の詳細な説明】

セキュリティ通信

本発明はセキュリティ通信の方法と装置に関する。

ディジタル方式の移動体音声通信システムは公知である。一例としてはＧＳＭ地上セルラーシステムがあり、他の例にはインマルサット（国際海事衛星機構）Ｍ衛星電話システム、（例えば欧州特許出願第０３６５８８５号に記載されている）イリジウム（商標）衛星セルラーシステム、（例えば英国特許出願第２２９５２９６号に記載されている）ＩＣＯ（商標）衛星セルラーシステム、または（例えば欧州特許出願第０５１０７８９号に記載されている）オデッセイ（商標）衛星セルラーシステムがある。

このようなシステムはワイヤレス・リンクを介して動作するので、無認可の人によって呼出しが傍受される危険がある。

ＧＳＭシステムには例えばドイツ郵政省、フランス・テレコムおよび通信大学から刊行されている１９８８年１０月１２～１４日のディジタル方式セルラー無線通信会議（ＤＣＲＣ）の議事録の第４ａ部に収録されているペーターＣ．Ｊ．ヴァン・デル・アーレント著の「ＧＳＭシステムにおけるセキュリティの側面と実施」に記載されているオプションの暗号方式を含んでいる。その詳細については下記のＧＳＭ推奨事項に記載されている。

ＧＳＭ０２．０９「セキュリティの側面」；ＧＳＭ０３．２０「セキュリティに関連する回線網機能」；ＧＳＭ０３．２１「セキュリティに関連するアルゴリズム」

このような方式では、認証センター（ＡｕＣ）として知られているデータベースが認証サービスの各加入者用の個々の暗号鍵番号（Ｋｉ）を保存しており、この鍵番号は加入者の移動体端末機に保持されている加入者情報モジュール（ＳＩＭ）と呼ばれるチップにも記憶されている。加入者はＳＩＭに記憶されたデータにアクセスできず、鍵を読取ることはできない。

セキュリティ・セッションが要求されると、乱数（ＲＡＮＤ）が認証センターによって生成され、顧客鍵（Ｋｉ）とともに、加入者への、また加入者からのメッセージを暗号化および暗号解読するセッション中に使用される暗号鍵（Ｋｃ）を計算するために使用される。

乱数はベース・トランシーバ局（ＢＴＳ）を経て加入者の移動体端末機に送られる。移動体端末機は乱数をＳＩＭに送り、これがＡ５と呼ばれるアルゴリズムを用いて暗号鍵Ｋｃを計算する。

このように、乱数は無線で送信されるが、顧客鍵Ｋｉあるいは暗号鍵Ｋｃは無線送信されない。

乱数および暗号鍵Ｋｃは当該の加入者に関わる詳細なデータを記憶するホーム・ロケーション・レジスタ（ＨＬＲ）データベースに送られ、更に現在使用中の領域用のビジティング・ロケーション・レジスタ（ＶＬＲ）にも送られ、かつ移動体端末機がそれを介して通信するＢＴＳに送られる。

移動体端末機およびベース・トランシーバ局内でＡ５暗号アルゴリズムを実施するために、現在のＴＤＭＡフレーム番号とともに暗号鍵Ｋｃが使用される。このように、個々のユーザー鍵Ｋｉは認証センターおよびＳＩＭだけに記憶されており、そこで暗号鍵Ｋｃが計算され、ＢＴＳおよび移動体端末機に送られる。

この方式は多くの側面では適切であるものの、無線送信経路を経由する場合のみ秘密保護を提供するので、完全なセキュリティをもたらすものではない。すなわち回線網の固定部分を改ざんすることによって違法にアクセスすることが可能である。

従って、本発明は端末同の暗号化を利用した移動体通信システムを提供する。暗号は無線経路だけではなく通信経路全体を経て１つのユーザー端末機から他のユーザー端末機に送られるので、プライバシー保護が改善される。

回線網を介した通信の端末間暗号化を行う際の基本的な問題点は、２人のユーザーの各々に同一の、すなわち相互間だけの秘密鍵を与えることにある。

ある用途では、（例えば全部を一人が所有している）端末機群は全てが同じ鍵にアクセスできる。それによってその端末機群を所有している以外の人に対するプライバシーは保たれるものの、群内の２つの端末機と群内の第３の端末機との通信のプライバシーは保証されないので、この解決方法は不完全なものである。

公開鍵暗号化システムを使用することも可能であり、その場合は各端末機が暗号解読秘密鍵と秘密ではない暗号化鍵を有しているので、第三者が誰でもデータを暗号化するために暗号化鍵を使用することができるが、暗号化公開鍵を使用して暗号化されたデータの暗号を受信者だけが解読することができる。

全てのユーザーにこのような一対の鍵が与えられ、一組のユーザー間の通信を準備する際に、各々のユーザーが相手に対して暗号解読鍵の秘密を保ったまま暗号化鍵を送信する通信システムを想定することもできよう。

しかし、通信回線網でこのような技術を利用することによって、何の監視の可能性もなく秘密の通信を完全に利用して犯罪者またはテロリストが通信できる可能性があることに対する公共上の関心が広まっている。

従って、本発明の側面では鍵のコピーを保存する“信頼できる第三者”データベースを提供し、かつそれぞれの端末機に他の端末機の鍵に関連する鍵データを配分することができる。

盗聴者による傍受を防止するために、好ましくは各端末機に送信された鍵データがマスキングされ、特に好ましくは受信側の端末機がまさに端末機の鍵を抽出、または解読できないようにする。その代わりに、好適な一実施の形態では、各端末機が独自の鍵と、他の端末機に関連して受信された鍵データとに複合的に依存した鍵を構成する。

好適な実施の形態では、マスキングは関数を利用して数字（この数字は各端末機鍵で同一である）とともに各端末機鍵を処理する形式を採用しているので、どの端末機も他の端末機の鍵を抽出できないが、各端末機が２つの鍵と数字の同じ組合わせを暗号化鍵として構成することができる。

本発明は衛星移動体ディジタル通信システムで使用されるように想定されており、また（例えばＧＳＭシステムのようなセルラーシステムにおけるような）対応する地上移動体ディジタル通信システムまたは固定リンク通信システムにも有用である。本発明はＥ－メールまたはインターネットのような蓄積・交換通信システムで実施してもよい。

本発明の側面とその好適な実施の形態は請求の範囲、および以下の詳細な説明に記載されている。

図面の簡単な説明

次に本発明の実施の形態を添付図面を参照しつつ例示目的でのみ説明する。

図１は本発明を実施した通信システムの要素を概略的に示したブロック構成図である。

図２は本発明での使用に適した移動体端末機の要素を概略的に示したブロック構成図である。

図３は図１の実施の形態の一部を形成する地上局ノードの要素を概略的に示したブロック構成図である。

図４は図１の実施の形態の一部を形成するゲートウェイ局の要素を概略的に示したブロック構成図である。

図５は図１の実施の形態の一部を形成するデータベース局の要素を概略的に示したブロック構成図である。

図６は図５のデータベース局の一部を形成する記憶内容を示した図である。

図７ａは図１の実施の形態の衛星によって放射されるビームを概略的に示した図である。

図７ｂは地球の周りの軌道内にある、図１の一部を形成する衛星の配置を概略的に示した図である。

図８は本発明の第１の実施の形態の、図２のハンドセットの構成要素間の信号の流れを示した構成図である。

図９は第１の実施の形態の、図１に示した構成要素間の暗号化データと信号との流れを示した概略構成図である。

図１０ａは第１の実施の形態の、図８に示したハンドセットの制御および暗号化の構成要素によって実行されるプロセスを概略的に示した流れ図である。

図１０ｂは第１の実施の形態の、図３の地上局の動作プロセスを概略的に示した流れ図である。

図１０ｃは第１の実施の形態の、図４の中央データベース局の動作プロセスを概略的に示した流れ図である。

図１０ｄは第１の実施の形態の、図８のハンドセット内に保持された加入者情報モジュール（ＳＩＭ）の動作プロセスを概略的に示した流れ図である。

図１１ａは図８の第１ハンドセット端末機による暗号化鍵の形成段階を示した図面である。

図１１ｂは第２ハンドセットでの暗号化鍵の形成プロセスを示した対応する図面である。

図１２は本発明の第３の実施の形態の、図１０ｃの動作を修正した流れ図である。

図１３ｂは第３の実施の形態の、図１０ｄの動作を修正した流れ図である。

図１４は本発明の第４の実施の形態でもたらされるセキュリティの段階を概略的に示した流れ図である。

図１５ａは本発明の第４の実施の形態に基づく、図８のハンドセットに備えられた機能素子の幾つかを概略的に示した構成図である。

図１５ｂは第４の実施の形態のデータベース局内に備えられた機能素子の幾つかを概略的に示した構成図である。

図１５ｃは第４の実施の形態の地上局内に備えられた機能素子の幾つかを概略的に示した構成図である。

図１６ａ（図１０ａに組込まれた部分である）は、第４の実施の形態に基づくハンドセットの動作を概略的に示した流れ図である。

図１６ｂ（図１０ｂに組込まれた部分である）は、第４の実施の形態に基づく地上局の動作プロセスを概略的に示した流れ図である。

図１６ｃ（図１０ｃに組込まれた部分である）は、第４の実施の形態に基づくデータベース局の動作を概略的に示した流れ図である。

図１６ｄ（図１０ｄに組込まれた部分である）は、第４の実施の形態に基づく加入者情報モジュールの動作を概略的に示した流れ図である。

発明の好ましい実施の形態

図１を参照すると、本実施の形態に基づく衛星通信回線網は移動体ユーザー端末機２ａ、２ｂと、軌道中継衛星４ａ，４ｂと、衛星地上局ノード６ａ、６ｂと、衛星システム・ゲートウェイ局８ａ、８ｂと、公衆交換通信回線網１０ａ、１０ｂと、固定通信端末機１２ａ、１２ｂとから構成されている。

衛星システム・ゲートウェイ８ａ、８ｂと地上局ノード６ａ、６ｂとの接続、およびノード６ａ、６ｂの相互接続を行うのはチャネル１４ａ、１４ｂおよび１４ｃからなる専用の地上回線網である。衛星４、地上局ノード６およびライン１４が移動体端末機２と通信するための衛星通信回線網の下部構造を構成し、かつゲートウェイ局８を介してアクセス可能である。

端末機所在データベース局１５は（例えば専用回線網のチャネル１４内の）信号リンク６０を介してゲートウェイ局と地上局６とに接続されている。

ＰＳＴＮ１０ａ、１０ｂは一般的には局所内ループ１８ａ、１８ｂを介して固定端末機１２ａ、１２ｂが接続されている局所内交換機１６ａ、１６ｂと、（例えば衛星リンクまたは海中光ファイバケーブル・リンクのような）国際横断リンク２１を介して相互に接続可能な国際交換センター２０ａ、２０ｂとから構成されている。ＰＳＴＮ１０ａ、１０ｂと固定端末機１２ａ、１２ｂ（例えば電話機）は公知であり、今日ではほぼ世界中で市販されている。

各々の移動体端末機は（この実施の形態では）、例えば（それぞれの場合に応じて）英国特許出願２２８８９１３号および英国特許出願第２２９３７２５号に開示されているような呼出しの開始時に割当てられる特定の周波数のＴＤＭＡタイム・スロットのようなダウンリンク・チャネルとアップリンク・チャネルからなる全二重チャネルを介して衛星４と通信する。この実施の形態では衛星４は静止衛星ではなく、従って周期的に１つの衛星４から別の衛星への引き継ぎが行われる。

＜移動体端末機２＞

図２を参照すると、図１の移動体端末機が示されている。

適切な形式の１つは図示のようなハンドセットである。ハンドセット２ａ、２ｂ等の詳細は本発明の一部を構成するものではなく、従来形のマイクロフォン３６と、スピーカ３４と、バッテリ４０と、キーパッド部３８と衛星通信に適した無線周波数（ＲＦ）インターフェース３２とアンテナ３１とともに、ディジタル・コーダ／デコーダ３０を備えた、ＧＳＭシステムで使用するのに現在使用できるものと同様のハンドセットでよい。好適には（例えば液晶ディスプレイのような）ディスプレイ３９も備えられている。ユーザー情報を記憶するスマートカード（ＳＩＭ）３５を受容する「スマートカード」読取り機３３も備えられる。

コーダ／デコーダ（コーデック）３０は誤り訂正コード化を行って毎秒４．８キロビットの伝送速度でコード化ビットストリームを生成するチャネル・コーダと、毎秒約３．６キロビットで会話ビットストリームを生成する低ビット伝送速度コーダとから構成されている。低ビット伝送速度コーダは例えば多重パルス予測コーダ（ＭＰＬＰＣ）、コードブック励起線形予測コーダ（ＣＥＬＰ）または残存励起線形予測コーダ（ＲＥＬＰ）のような線形予測コーダでよい。あるいは、サブバンド・コーディングのようなある種の形式の波形コーディングを用いてもよい。

採用される誤り訂正コード化にはブロック・コード、ＢＣＨコード、リードーソロモン(Reed-Solomon)コード、ターボ・コードまたは重畳コード（convolutionalcode）を用いてもよい。同様にコーデック３０は（例えばViterbi、すなわちソフト決定コード化を用いた）対応するチャネル・デコーダと音声デコーダとからなっている。

更に適切にプログラムされたマイクロプロセッサ、マイクロコントローラ、またはディジタル信号プロセッサ（ＤＳＰ）チップからなる制御回路３７（これは実際にはコーダ３０と統合されてもよい。）も備えられている。

ＳＩＭ３５は、好ましくはＧＳＭ推奨事項０２．１７「加入者識別モジュール」および１１．１１に準拠するものであって、好ましくは工業規格「スマートカード」として実施される。従ってＳＩＭ３５と読取り機３３とは、好ましくは国際規格ＩＳＯ７８１０、７８１１および７８１５に記載されているようなものである。これらの規格、およびＧＳＭ０２．１７および１１．１１は全て本明細書に参考文献として組入れられている。

具体的には、ＳＩＭ３５はプロセッサ３５ａと永久メモリ（ｐｅｒｍａｎｅｎｔ　ｍｅｍｏｒｙ）３５ｂとを含んでいる。プロセッサ３５ａは後に詳述するように、ある種の暗号化機能を行うように構成されている。

＜地上局ノード６＞

地上局ノード６は衛星と通信するように構成されている。

地上局ノード６は図３に示すように、少なくとも１つの移動衛星４を追跡するように構成された少なくとも１つの衛星追跡アンテナ２４と、アンテナ２４に信号を送るためのＲＦパワー増幅器２６ａと、アンテナ２４から信号を受信するためのＲＦパワー増幅器２６ｂと、衛星位置推定データを記憶し、アンテナ２４の操舵を制御し、かつ（アンテナ２４を介して衛星４に信号を送ることによって）必要な衛星４の制御を行う制御装置２８とからなる従来形の衛星地上局２２から構成されている。

地上局ノード６は更に、専用回線網の一部を形成する中継リンクに接続された回線網スイッチ４４からなる移動衛星交換センター４２を備えている。マルチプレクサ４６は、スイッチ４４から交換された呼出しを受信し、それらを合成信号に多重化して、低ビット伝送速度の音声コーデック５０を介して増幅器２６に供給するように構成されている。最後に、地上局ノード６はノード６がそれと通信する衛星４のサービス領域内の各移動体端末機２ａの詳細なデータを記憶する局所内記憶装置４８を備えている。

＜ゲートウェイ８＞

図４を参照すると、ゲートウェイ局８ａ、８ｂは、この実施の形態ではＧＳＭシステムのようなディジタル方式の移動体セルラー無線システムで使用される種類の市販の移動体交換センター（ＭＳＣ）から構成されている。あるいは、ゲートウェイ局はソフトウェア制御で回線網１０を衛星システムの中継線１４と接続するように動作するＰＳＴＮ１０ａ，１０ｂの１つを形成する国際交換機、またはその他の交換機の一部から構成されていてもよいであろう。

ゲートウェイ局８はＰＳＴＮ１０から入るＰＳＴＮ線を制御装置７２の制御で、１つ以上の地上局ノード６に接続された専用のサービス線１４と相互に接続するように構成されたスイッチ７０を備えている。制御装置７２は信号装置７４を介してデータベース局１５に接続されたデータ・チャネル６０と通信することができ、かつある種の適切な様式（例えばパケットまたはＡＴＭセル）でデータ・メッセージを生成するように構成されている。

ゲートウェイ局８にはゲートウェイ局８がそのためのホーム・ゲートウェイ局である移動体端末機２に関する勘定、サービスおよびその他の情報を記憶する記憶装置７６も備えられている。データは、ＰＳＴＮ１０、または衛星回線網を構成する地上局ノード６から信号装置７４またはスイッチ７０を介して受信された後、制御装置７２によって記憶装置７６に書込まれる。この記憶装置は地上ＧＳＭ回線網のビジティング・ロケーション・レジスタ（ＶＬＲ）と同様に機能し、従って市販されているＶＬＲを記憶装置７６として使用してもよい。

衛星システム中継線１４はこの実施の形態では、信号の劣化および遅延の最小限の許容基準を満たす高性能の専用回線からなっている。この実施の形態では、回線１４は全て地上リンクからなっている。中継線１４は好適には専用回線であるので、回線１４は回線網１０への物理的チャネルの別個のセットを形成する。しかし、回線網１０を経た仮想回路を使用しても構わない。

＜データベース局１５＞

図５を参照すると、データベース局１５はディジタル・データ記憶装置５４と、信号発信回路５６と、信号発信回路５６と記憶装置５４とに接続されたプロセッサ５８と、データベース局１５をゲートウェイ局８と地上局６とに接続する信号発信またはデータ・メッセージ通信用の衛星システム回線網を構成する信号リンク６０とからなっている。

記憶装置５４は全ての加入者端末機２毎に、識別名（例えば国際移動体加入者識別名、すなわちＩＭＳＩ）を示す記録、端末機２の現在の状態（後に詳述するようにそれが「局所内」であるか「大域的」であるか）、（座標の形状で、またはそれがある領域を特定するコードとしての）移動体端末機２の地理的な位置、（単一のポイントで勘定その他のデータを収集できるように）装置がそれによって登録されている「ホーム」ゲートウェイ局８、および装置２がそれによって衛星４を介して通信する現在稼動中の地上局ノード６を含んでいる。記憶装置の内容は図６に示してある。

更に、この実施の形態では記憶装置は、各ユーザー毎に後述のように使用される一意的、かつ固有の暗号化鍵Ｋｉを記憶している。

信号装置５６とプロセッサとはゲートウェイ８またはノード６から（パケット切換え接続でよい）信号送信回路６０を経て、（例えば端末機２の電話番号のような）移動体端末機２の１つを特定するデータからなる呼び掛けデータ・メッセージを受信するように構成されており、プロセッサ５８は端末機２の状態および稼動中の地上局ノード６に関して記憶装置５４を探索し、かつこれらのデータをデータ回線６０を経て応答メッセージで送信するように構成されている。

このように、この実施の形態ではデータベース局１５はＧＳＭシステムのホーム・ロケーション・レジスタ（ＨＬＲ）と、ＧＳＭシステムの認証センター（ＡｕＣ）の両方の機能を果たすように動作しており、かつ市販のＧＳＭ製品を使用してもよい。

＜衛星４＞

基本的に衛星４ａ、４ｂは公知のヒューズＨＳ６０１型のような従来形の通信衛星からなっており、英国特許出願第２２８８９１３号に開示されているようなものでよい。各々の衛星４は衛星の下方の足跡をカバーするビーム・アレイを発生するように構成されており、各々のビームは英国特許出願第２２９３７２５号に記載され、図７ａに図示したような多数の異なる周波数チャネルとタイム・スロットとを含んでいる。

衛星４ａは地球全体をカバーするため（好ましくは大域的にカバーするため）充分な数の星座内に適当な軌跡で配置され、例えば１０の（またはそれ以上の）衛星を例えば図７ｂに示すように１０，５００キロメートルの高度で２つの（またはそれ以上の）互いに直交する中間円形軌道で備てもよい。しかし、欧州特許出願第０３６５８８５号、または例えばイリジウムシステムに関するその他の刊行物に開示されているように、それ以上の数の低高度の衛星を使用してもよい。

＜登録とロケーション＞

一実施の形態では、顧客の移動体端末機２は２つの異なる状態の一方で登録できる。すなわち、移動体端末機が１つの局所すなわち衛星システム回線網の一部を介してのみ通信できる“局所内”状態と、衛星システム回線網のどの部分を介してでも通信できる“大域的”状態である。

各々の装置２の状態（すなわち“局所内”または“大域的”）はデータベース局１５の記憶装置５４に装置２用に保存される記録に記憶される。

移動体端末機２は、次の各場合すなわち端末機２が発呼用に使用された時、および（または）端末機２がスイッチ・オンされた時、および（または）端末機がスイッチ・オンの状態の間に周期的にセルラー地上通信の分野で公知である自動登録プロセスを実行する。従来のとおり、登録プロセスは（例えば電話番号を共通の呼び掛け、もしくは信号通信周波数で送信することによって）移動体端末機２を特定する信号通信の形式をとる。

送信された信号は１つ以上の衛星４によってピックアップされる。通常の状況では、信号は複数の衛星４によってピックアップされ、受信された信号強度および（または）到着時間が移動体端末機２と信号を受信する衛星４の識別名とともに、衛星４が通信しているの地上局ノード（単数または複数）６および信号線６０を経てデータベース局１５に送信される。

データベース局１５のプロセッサ５８は例えば到着時間差に応じて移動体端末機２の地上位置を計算して、この位置はデータベース５４内に記憶される。移動端末機２と通信するのに最適な地上局ノード６（“能動局”）の識別名も記憶される。これは一般に、記憶された端末機２の位置と記憶された各々の地上局ノード６の所定位置とを比較し、最も近い位置を選択するプロセッサ５８によって特定される。しかし、また、あるいはその代わりに、衛星４を介して受信された信号の強度、または（回線網の混雑のような）その他の要因を考慮して、ボーダーラインの場合は、移動体端末機２に地理的にさほど近くはない地上局ノードを結果として選択してもよい。次に割当てられた能動地上局ノード６の識別名は同様に記憶装置５４内でその端末機用の記録に記憶される。

＜呼出しの準備と経路指定＞

移動体端末機２への、または移動体端末機からの呼出しの経路指定プロセスは、双方とも本明細書に完全に組入れられている英国特許出願第２２９５２９６号またはＰＣＴ／英国特許第９５０１０８７号に詳細に記載されている。簡略に説明すると、領域外の局所内ユーザー向けには、ユーザーへの、またはユーザーからの呼出しはデータベース局に持ち込まれ、この局はユーザーが局所外にあることを判定すると、その後は呼出しを処理しない。上記の英国および国際出願に記載されている好適な実施の形態では、領域内にある局所内のユーザー向けには、ユーザーへの、またはユーザーからの呼出しは能動地上局６、地上回線網、および国際公衆交換局回線網（ＰＳＴＮ）を経て衛星リンクを介して最も近いゲート

ウェイ８から地上のユーザーに送られるように準備される。

大域領域のユーザー向けには、呼出しは衛星と能動地上局を経て、次に地上回線網を経て地上のユーザーに最も近いゲートウェイ局８に経路指定される。

移動端末機のユーザーに割当てられるダイアル番号には衛星サービス回線網に対応するコードを後に付した“国際”の接頭辞を有していてもよい。あるいは、衛星サービスに割当てられた地区コードを後に付した国際接頭辞を有していてもよいであろう。

１つの端末機のユーザーと別の端末機のユーザーとの間の呼出しは信号を第１の衛星リンクを経て第１の移動体端末機のユーザーの能動地上局ノードへと下ろし、地上回線網を経て（第１の移動体端末機の地上局ノードと同一でもよいが、必ずしもそうではなくてもよい）第２の移動体端末機のユーザーの能動地上局へと向け、次に（同じ衛星を介してでもよいが、そうでなくてもよい）第２の衛星リンクを経て第２の端末機のユーザーへと向けられる。

＜第１の実施の形態＞

図８は図２の移動端末機の素子を経た信号の流れをより詳細に示している。アンテナ３１から受信された信号はＲＦモデム３２によってＲＦ復調され、暗号化モードの場合は例えばＳＩＭ３５から供給される暗号解読鍵に従ったＡ５アルゴリズムを用いて受信データを解読するように構成されたプロセッサ回路３７に送られる。暗号解読鍵はＫａ.ｂと呼ばれる。

解読されたビットストリームは次にチャネルコーデック３０ｂに送られ、これが誤り訂正デコードを行い、誤り訂正された音声信号がディジタル／アナログ変換器を含むビット伝送速度が低いコーデック３０ａに供給され、そのアナログ出力がスピーカ３４に送られる。

マイクロフォン３６からの音声はアナログ／ディジタル変換器を含むビット伝送速度が低いコーデック３０ａに送られ、その結果生じるビット伝送速度が低い音声信号はチャネルコーデック３０ｂによって誤り訂正を含むようにコード化される。誤り訂正されたビットストリームは暗号化モードにある場合には次に制御回路３７によって暗号化され、暗号化されたビットストリームはアンテナ３１から送信されるようにＲＦモデム３２に送られる。

ステップ１２１０で、中央データベース局１５は信号通信回線網６０と、それぞれの地上局６ｂおよび６ａと、衛星４ｂと４ａとを経て第１部分鍵（Ｋpa）を第２端末機２ｂに送信し、第２部分鍵（Ｋpb）を第１端末機２ａに送信する。

この段階で、個々の端末機鍵は乱数ＲＡＮＤとの排他的ＯＲ演算によって既に“スクランブル”されている。部分鍵の１つを傍受する無認可の盗聴者は２つの未知要素、すなわち乱数ＲＡＮＤと端末機鍵とに直面するのでそれから端末機鍵を知ることはできない。双方の部分鍵を傍受する無認可の盗聴者でも３つの未知の要素をそこから導き出すデータを２つしか持っていないので、乱数または端末機鍵のうちの１つのいずれかを導き出すことはできない。たかだか導きだせるのは２つの端末機鍵の差異であり、これには価値がない。

ここで図１０ｂを参照すると、ステップ１１０６で各地上局は部分鍵を受信し、ステップ１１０８でこれを移動体端末機へと送る。

図１０ａを参照すると、ステップ１００４で各々の移動体端末機は対応する部分鍵を受信する。ステップ１００６で、部分鍵はカード読取り機３３を介してＳＩＭ３５に送信される。

図１０ｄを参照すると、ステップ１３０２で、ＳＩＭは部分鍵を受信し、ステップ１３０４でＳＩＭはメモリ３５ｂ内から端末機鍵を読出す。ステップ１３０６で、ＳＩＭプロセッサ３５ａは受信した部分鍵と記憶されている端末機鍵とでビット方式の排他的ＯＲ演算を行うことによって暗号化鍵を計算して、新たな１２８ビットのバイナリ数を生成する。ステップ１３０８で、ＳＩＭ３５はそのようにして計算された（Ｋa，Ｋbと呼ばれる）暗号化鍵をカード読取り機３３を経て端末機プロセッサ３７に供給する。

第１端末機２ａに送られた部分鍵が第２端末機２ｂの端末機鍵Ｋbと乱数ＲＡＮＤとの排他的ＯＲ関数の積（Ｋpb＝Ｋb＋ＲＡＮＤ）であることが想起されよう。このように、図１０ａに示すように、ステップ１３０６で、この部分鍵Ｋpbと端末機鍵Ｋaとの排他的ＯＲ演算の積として計算された暗号化鍵はＫab＝Ｋb＋ＲＡＮＤ＋Ｋaである。

同様に、図１０ｂに示すように第２端末機２ｂでは、計算された暗号化鍵Ｋabは部分鍵Ｋpaと端末機鍵Ｋbとの排他的ＯＲ演算の積である。言い換えると、Ｋab＝Ｋa＋ＲＡＮＤ＋Ｋbである。

図９、１０および１１を参照して、通信の暗号化モードを準備するプロセスをより詳細に説明する。

２つのユーザー端末機２ａと２ｂ間の通信セッション中は、一方または双方の端末のユーザーは暗号形式で会話を継続するように選択する。従って、図１０ａを参照すると、ステップ１００２で呼出し側はキーボード３８によるキー・ストロークのシーケンスに入り、これがプロセッサ３７によってセキュリティに関わる命令として認識され、従ってプロセッサ３７はステップ１００２で帯域内または関連する制御チャネルでの暗号化に関わる信号を送信する。

図１０ｂを参照すると、地上局６で、ステップ１１０２ではプライバシー要求信号が受信され、ステップ１１０４で信号は（端末機２ａおよび２ｂの識別名を示す識別コードとともに）中央データベース局１５に、また第２のユーザー端末機２ｂに同時に送信される。

第２ユーザー端末機２ｂでは、プライバシー信号の受信は図１０ａのステップ１００２で行われる。

図１０ｃを参照すると、ステップ１２０２においてプライバシー信号が中央データベース局で受信される。

ステップ１２０４で、データベース局１５のコントローラ５８がメモリ５４にアクセスし、第１移動体端末機２ａ用に記憶された個々の暗号化鍵Ｋaと、第２移動体端末機２ｂ用に記憶された鍵Ｋbとを読出す。

ステップ１２０６で、コントローラ５８は疑似乱数（ＲＡＮＤ）を生成する。

この実施の形態では、鍵ＫaとＫbとはそれぞれ１２８ビットのバイナリ数であり、乱数ＲＡＮＤは別の１２８ビット・バイナリ数である。

ステップ１２０８で、コントローラ５８は第１と第２の部分鍵ＫpaとＫpbとを計算する。第２部分鍵の計算は図１１ａに示されている。この計算で１２８ビットの数が生成され、その各ビットは第２端末機鍵Ｋbの対応位置内のビットと乱数ＲＡＮＤとの排他的ＯＲ関数である。このように、第２部分鍵ＫpbはＫb＋ＲＡＮＤに等しい（但し、＋はバイナリ数の排他的ＯＲ演算を示す）。

第１部分鍵Ｋpaは図１０ｂに示すように、第１端末機鍵Ｋaと乱数ＲＡＮＤとのビット毎の排他的ＯＲ演算を行うことによって全く同様に計算される。

排他的ＯＲ演算は関連する数学的法則に従うので、これら２つの計算結果は同一である。言い換えると、各端末機は同じ暗号化鍵を計算する。

図１０ａを再び参照すると、ステップ１００８で端末機プロセッサ３７は暗号化鍵Ｋabを受信し、ステップ１０１０で端末機３７は暗号化モードに切り換わる。その後、ステップ１０１２に示すように、プロセッサ３７はＲＦ変調および送信の前にコーデック３０からのビットストリームを暗号化し、かつＲＦモデム３２からの対応するビットストリームをコーデック３０に送られる前に解読する機能を果たす。

暗号化アルゴリズムは任意の適宜のアルゴリズムでよく、（暗号化鍵自体が秘密であるので）オープンに知られてもよい。特に、暗号化アルゴリズムはＧＳＭハンドセットで用いられ、前述の推奨事項に記載されているＡ５暗号化アルゴリズムであることが便利である。これはほとんどのＧＳＭハンドセットに既に内蔵されている。

このように、要約すると図９に示すように、この実施の形態では各端末機２は端末機、および中央データベース局１５内に備えられたＳＩＭ３５内に記憶された関連する一意的な端末機鍵を有している。使用される暗号化鍵は双方の端末機鍵の関数である。データベース局１５は一方の端末機２に他方の端末機の端末機鍵を配分する。

端末機鍵はマスキングされた形式で配分される。この実施の形態におけるマスキングは乱数との排他的ＯＲ演算の形式を呈している。演算は各端末機で行われてその独自の端末機鍵をマスキングされた他の端末機鍵と結合する演算により各端末機で双方の端末機鍵の同一の関数である暗号化された端末機鍵を生成する。この端末機鍵はこの実施の形態では同じ端末機番号に従って各端末機鍵を処理することによって便利に構成される。

端末機鍵をマスキングされた形式で送信することによって、盗聴者がいずれかの端末機鍵へのアクセス手段を得ることが防止される。（例えば疑似乱数の順序を継続的に変えることによって）各セッションの演算でのマスキングを変更することで、盗聴者が時間をかけてマスキング関数を知ることは不可能である。

他の端末機鍵は端末機自体からもマスキングされているので、端末機またはＳＩＭのいずれかが他の端末機鍵を解読することも不可能である。

最後に、ＧＳＭシステムの場合のように端末機はそれ自体の端末機鍵を知らない。何故ならば、これは端末機からのアクセスが不可能であるＳＩＭに記憶されているからであ。このことが重要であるのは、そうしないと基本的に一方の端末機が他方の端末機に送信された部分鍵を聞くことができ、それ自体の端末機鍵を知って、乱数を導き出した後、送信された部分鍵から他の端末機鍵を解読できるからである。

＜第２の実施の形態＞

第２の実施の形態では、中央データベース局で不正を企てる機会を減らすことによってセキュリティは更に改善される。第２の実施の形態は、図１１に示すように図１０ｃのステップ１２０４から１２１０の代わりにステップ１４０４から１４２０までが実行される点を除いては第１の実施の形態とほぼ同様に動作する。

従って、ステップ１２０２の後、プロセッサ５８は先ずステップ１４０４で第１端末機鍵Kaにアクセスし、次に（ステップ１２０６に関して前述したように）ステップ１４０６で乱数を計算し、次に（ステップ１２０８に関して前述したように）ステップ１４０８で第１部分鍵を計算し、次に（ステップ１２１０に関連して前述したように）ステップ１４１０で第１部分鍵を送信する。

これらの動作の後、局所的に記憶されているKaとKpaのコピーが消去される。次に、ステップ１４１４で、プロセッサ５８は第２端末機鍵Kbにアクセスし、第２部分鍵を計算し（ステップ１４１６）、第２部分鍵を送信し（ステップ１４１８）、かつ第２部分鍵と第２端末機鍵とを消去する（ステップ１４２０）。

このようにして、この実施の形態では２つの部分鍵と端末機鍵へのアクセスは時間的に分離され、データベース局１５を盗聴したり不正使用する可能性が減少する。

２つの部分鍵および（または）端末機鍵へのアクセスは他の方法でも分離できるのは明白であろう。例えば、２つの端末機鍵を物理的に分離された装置に送信し、次に乱数をそこで端末機鍵を結合するために各装置に送信する。

なわれ、更に別の暗号化データを記憶する必要がないようにする。

しかし、明らかに他の形式の暗号化も可能である。すなわち、追加の乱数も送出されるより精巧な暗号化アルゴリズムを用いることが可能であろう。最後に、この実施の形態で説明した暗号化方式を用いる場合、端末機鍵のマスキングによって生成される部分鍵ではなく送信された端末機鍵を直接暗号化することも可能であろう。それによって、受信された端末機鍵がＳＩＭ３５内でだけ解読されるので、ほとんどの状況でより高いレベルのセキュリティが得られよう。しかし、不正なＳＩＭが製造されるような危険がある場合は、それによってＳＩＭからも他の端末機鍵の識別名が隠されるので、部分鍵を生成するためにマスキングが使用される。

＜第４の実施の形態＞

この実施の形態では、ＧＳＭ互換性回線網に備えられ、前記のＧＳＭ推奨事項に記載されているエアインターフェース暗号化および認証・システムと組合わせて第１の実施の形態の原理が採用される。

図１４を参照すると、セキュリティ機能は以下の順序で与えられる。すなわち、

認証（ステップ２００２）、エアインターフェース暗号化（ステップ２００４）、端末間暗号化（ステップ２００６）である。

基本的には、最初の２ステップは既存のＧＳＭ回線網の場合と同様であり、第３のステップは第１の実施の形態に関して前述したステップと同様である。しかし、明確にするため、以下に更に説明を加える。

図１５ａを参照すると、ハンドセット・プロセッサ３７とＳＩＭ３５とによって実行される機能が別個の機能ブロックとして説明される。各機能ブロックは勿論、別個のマイクロプロセッサまたはディジタル信号プロセッサ（ＤＳＰ）によって実行することもできるが、この実施の形態では、実際には上記のプロセッサ装置はハンドセット内に１つと、ＳＡＮ３５内に１つしか備えられていない。

図１５ａを参照すると、アンテナ３１から受信され、ＲＦモデム３２によって復調された信号はエアインターフェース暗号化鍵Kcに従ってＧＳＭから公知のＡ５アルゴリズムを適用するように構成された第１の暗号化／暗号解読段３７２

同じ乱数を２つの別の装置に送信するのではなく、セキュリティを更に高めるために同一の２つの乱数発生器を異なる２つのロケーションに段階的に備え、そこに２つの端末機鍵を送信してもよい。このように、２つの端末機鍵および（または）部分鍵へのアクセスを物理的および、またはその代わりに時間的に分離してもよい。

＜第３の実施の形態＞

上記の実施の形態では、部分鍵Kpa、Kpbが暗号化されずに普通文で送信される。この実施の形態では、各送信毎に暗号化が行われることによってセキュリティは更に高まる。

共通の暗号を用いることも可能だろうが、共通の暗号にアクセスする（例えばプライバシー・サービスを認可された他のユーザーのような）盗聴者が暗号を解読できる可能性があるので、それは好ましくない。

同様に、ＧＳＭシステムで公知の種類のエアインターフェース暗号を利用することは、それによって回線網の固定部分での傍受に対してオープンになるので好ましくない。

従って、この実施の形態では、ＳＩＭ３５は（ＧＳＭシステムで用いられるＡ５アルゴリズムであることが便利な）暗号解読アルゴリズムを記憶しており、かつデータベース局１５は対応する暗号化アルゴリズムを実行するように構成されている。

図１３ａを参照すると、この実施の形態では第１の実施の形態の図１０ｃのプロセスはステップ１２０８と１２１０の間にステップ１２０９を含めるように修正されている。このステップでは、各部分鍵はそれが送出されるべき端末機の端末機鍵を用いて暗号化され、暗号化された形式で送信される。

図１３ｂを参照すると、この実施の形態では各端末機でＳＩＭプロセッサ３５ａはステップ１３０４と１３０６との間で追加のステップ１３０５を実行する。ステップ１３０５で、受信された部分鍵は暗号化鍵を計算する前に端末機鍵を用いて解読される。

このように、この実施の形態では、送信された部分鍵を暗号化することによってセキュリティが更に高まる。暗号化が宛先の端末機の端末機鍵を利用しておこと、端末間暗号鍵Ka.bに従って暗号解読する（この場合もＧＳＭシステムで使用され、上記の推奨事項に記載されているＡ５アルゴリズムであることが便利である）第２暗号解読アルゴリズムを適用するように構成された第２暗号化／暗号解読段３７４とを通過する。暗号解読されたビットストリームはその後でコーデック３０に供給される。

同様にして、コーデック３０からの会話ビットストリームは逆の順序で２つの暗号化／暗号解読段３７２、３７４を通過する。図面を明解にするため、信号経路は図１５ａでは省略してある。

ＳＩＭ３５内には端末機用の端末機鍵Kiを記憶するための端末機鍵記憶レジスタ３５２が配設されている。端末機鍵記憶レジスタ３５２は端末機鍵Kiを符号定数計算段３５４に送るように接続されており、この段は前述のＧＳＭ推奨に記載され、ＧＳＭシステムで使用されているＡ３アルゴリズムに従って、端末機を認証するために用いられる“符号付き応答”数（ＳＲＥＳ）を計算するように構成されている。応答計算段３５４はカード読取り器３３を介してＲＦモデム３２から出力される暗号化されないビットストリームから乱数（ＲＡＮＤ１）を受信するようにも接続されている。

端末機鍵・レジスタ３５２は端末機鍵Kiを第１鍵生成段３５６に送るようにも接続されており、この段も乱数（ＲＡＮＤ１）を受信し、かつそこから上記のＧＳＭ推奨事項に記載され、ＧＳＭシステムで使用されているＡ８アルゴリズムに従ってエアインターフェース暗号化鍵Kcを計算するように構成されている。このようにして計算された鍵はカード読取り器３３を介して端末機プロセッサ３７の第１の（エアインターフェース）暗号化／暗号解読段３７２に送られる。

端末機鍵・レジスタ３５２は端末機鍵を第２鍵生成段３５８に送るようにも接続されており、この段は端末機プロセッサ３７の第１の（エアインターフェース）暗号化／暗号解読段３７２の解読された出力から（カード読取り器３３を介して）受信するように接続された端末機鍵Kiと部分鍵Kpbを利用して（上記の第１の実施の形態で説明したような）端末機間暗号化用の暗号化鍵Kabを生成するように構成されている。

このようにして計算された端末機間暗号化鍵は端末機プロセッサ３７の第２の

（端末機間）暗号化／暗号解読段３７４に送られる。

図１５ｂを参照すると、中央データベース局は、この実施の形態ではそれぞれの使用機会に無作為の順序で新たな１２８ビットのバイナリ数（ＲＡＮＤ１）を生成するように構成された乱数発生器５８２と、端末機鍵Ｋｉを記憶する記憶装置５４と、記憶装置５４からの端末機鍵と乱数（ＲＡＮＤ１）とを受信し、かつそこから（上記のＧＳＭ推奨事項に記載され、ＧＳＭシステムで使用される）Ａ８アルゴリズムに従ってエアインターフェース暗号化鍵Ｋｃを計算するように接続された鍵生成段５８４と、これも同様に端末機鍵と乱数とを受信するように接続され、（上記のＧＳＭ推奨事項に記載され、ＧＳＭシステムで使用される）Ａ３アルゴリズムに従って符号付きの応答数（ＳＲＥＳ）を計算するように構成された、符号定数計算段５８６とから構成されている。

乱数発生段５８２と、符号付き応答発生段５８６と、鍵生成段５８４との出力は地上局６に送信されるように信号通信回路５６に接続されている。

図１５ｃを参照すると、地上局６は（データベース４８内に）それぞれがデータベース局１５から信号通信回路６０を経て送信される乱数と、対応する符号付き応答（ＳＲＥＳ）と、対応するエアインターフェース暗号化鍵（Ｋｃ）とからなる所定数（例えば５つ）を記憶するように構成されたトリプレット・レジスタ４８２とから構成されている。

移動体端末機２が地上局６に登録される機会毎に、地上局は中央データベース局１５から所定数のトリプレットが供給されることを要求し、中央データベース局はそれに従って所定数のトリプレットを発生し、信号通信チャネル６０を経てこれらのバイトがレジスタ４８２内に記憶されるように送信する。

地上局６内には地上局６のトリプレット・レジスタ４８２およびエアインターフェース部品２４、２６に結合され、移動体端末機２から受信した符号付き応答（ＳＲＥＳ）数とレジスタ４８２内に記憶された符号付き応答とを比較し、かつ２つの数の対応関係の有無を示すように構成された比較器２８２が備えられている。２つの数が対応しない場合は、ユーザーは認証されず、制御装置２８によってサービスが中断される。

最後に、地上局６はトリプレット・レジスタ４８２から送られたエアインターフェース暗号化鍵Ｋｃを利用して（ＧＳＭから公知である）Ａ５アルゴリズムに従って暗号化と暗号解読を行うように構成されたエアインターフェース暗号化段２８４を備えている。

暗号化方向では、エアインターフェース暗号化／暗号解読段２８４はコーデック５０からの入力を受け、その出力をエアインターフェース部品２４、２６に送る。一方、暗号解読方向では、暗号化／暗号解読段２８４はその入力をエアインターフェース部品２４、２６から受け、その出力をコーデック５０に送る。

ここでこの実施の形態の動作を図１６ａから１６ｄを参照してより詳細に説明する。図１６ａから１６ｄには図１０ａから１０ｄの処理段階が組入れられており、後述で更に詳細に説明することはない。

図１０ａでは、先ずプライバシー要求が一方の通話者から出され、プライバシー要求信号が端末機２ａから送信される。

プライバシー信号が地上局６ａで受信され（ステップ１１０２）、それがデータベース局１５に送られた（ステップ１１０４）後、図１６ｃに示すようにステップ１２０２と１２０４が実行され、２つの端末機の端末機鍵が導出される。

次に、ステップ１２０５で、双方の加入者が端末機間の暗号化を利用する権利があるか否かを判定するテストが行われる。権利がある場合は、図１０ｃのステップ１２０６から１２１０が実行される。引き続いて、または、権利がない場合は、データベース局１５はステップ１２１２に進み、そこでデータベース局は地上局（単数または複数）６ａ、６ｂに、２つの端末機２ａ、２ｂに対して端末機認証のチェックを行い、かつエアインターフェース暗号化を開始するように命令する信号を送信する。

図１６ｂに戻ってこれを参照すると、各地上局６は命令信号と部分鍵を受信すると（ステップ１１１０）、トリプレット・レジスタ４８２から得た次の乱数ＲＡＮＤ１を含む認証呼び掛けメッセージを送信する（ステップ１１１２）。加えて、ＧＳＭシステムの場合と同様に、次の確認のために鍵ナンバーを送信してもよい。

図１６ａを参照すると、認証要求メッセージを受け取ると（ステップ１０１４）、乱数（ＲＡＮＤ１）が抽出され、ＳＩＭ３５に送出される。（ステップ１０１６）。

図１６ｄを参照すると、ＳＩＭ３５で、乱数ＲＡＮＤ１を受信すると（ステップ１３１０）、ＳＩＭプロセッサ３５ａは端末機鍵Ｋａを探索し（ステップ１３１２）、Ａ３アルゴリズムを用いて符号付き応答（ＳＲＥＳ）を計算する（ステップ１３１４）。

ステップ１３１６で、ＳＩＭプロセッサ３５ａは乱数（ＲＡＮＤ１）と端末機鍵Ｋａを用いてエアインターフェース暗号化鍵Ｋｃを計算する。ステップ１３１８で、ＳＩＭ３５は符号付き応答数（ＳＲＥＳ）とエアインターフェース暗号化鍵（Ｋｃ）をカード読取り器３３を経て端末機プロセッサ３７に送信する。

引き続いて、ＳＩＭ３５は図１０ｄのプロセスを実行する。

図１６ａを参照すると、符号付き応答数（ＳＲＥＳ）をステップ１０１８で受信した後、端末機プロセッサ３７はＳＲＥＳ数を地上局６ａに送信する（ステップ１０２０）。

図１６ｂを参照すると、地上局６は符号付き応答数を受信し（ステップ１１１４）、これとトリプレット・レジスタ４８２内に保存されている記憶された符号付き応答数とを比較する（ステップ１１１６）。

２つが一致しない場合は、呼出しは終了する（ステップ１１１７）。あるいは、必要ならば更に認証の試みがなされてもよい。

移動体端末機２から受信された符号付き応答がステップ１１１６で記憶された符号付き応答と一致した場合は、地上局６は受信されたばかりの符号付き応答に対応するトリプレット・レジスタ４８２に記憶された暗号化鍵Ｋｃを読取り、暗号化鍵ＫｃとともにＡ５アルゴリズムを用いて移動体端末機２へのそれ以降の全ての交信の暗号化と、移動体端末機からのそれ以降の全ての交信の暗号解読を開始する（ステップ１１１８）。ＧＳＭシステムでは一般的であるように、暗号化アルゴリズムへの入力としてフレーム数を使用してもよい。

その後、地上局６は図１０ｃのステップ１１０８に戻り、データベース局１５から受信した部分鍵を端末機２に送信するが、この実施の形態ではこれは暗号化された形式で行われる。

図１６ａに戻ってこれを参照すると、ＳＩＭ３５からのエアインターフェース暗号化鍵Ｋｃを受信すると（ステップ１０２２）、端末機プロセッサ３７は暗号化／暗号解読モードを開始し、このモードではエアインターフェース・モデム３２から受信された交信は全て暗号解読され、エアインターフェース・モデム３２に送信された交信は全てＡ５アルゴリズムとエアインターフェース暗号化鍵Ｋｃとを用いて暗号化される。地上局６が補足的にフレーム数を用いる場合は、端末機２も同様にこれを用いる。

端末機プロセッサ３７によって実行されるプロセスは次に図１０ａのステップ１００４に戻って、地上局６から受信した部分暗号化鍵Ｋｐｂを（暗号形式で）受信し、暗号解読し、かつ利用する。

上記の説明ではどの端末機も最近は認証されておらず、またどの端末機も既にエアインターフェース暗号化モードには入っていないものと想定されているが、かならずしもそういう場合だけではないことが理解されよう。いずれかの端末機が既にエアインターフェース暗号化を適用している場合は、認証および空気インターフェース暗号化を準備するための前述の対応するステップが再び実行されることはない。

上記の実施の形態では、補足的な防護策を講じてもよい。たとえば、セキュリティ通信を開始するため、ＳＩＭに保存されているデータと突き合わせるために、端末機のユーザーにＰＩＮコードを入力することを要求してもよい。

本発明がＧＳＭ互換性システムまたはその類似システムで実施される場合は、ＳＩＭ３５は国際移動体端末機加入者識別番号（ＩＭＳＩ）の形式の更に別の情報と、場合によっては迅速ダイアリングおよびその他の目的のための電話番号のリストを含んでいることが理解されよう。

本発明は、それぞれが対応する閉鎖的ユーザー・グループ（ＣＵＧ）を指定するリストをデータベース局１５に保存することによって便利に実施される。それによって１つの閉鎖的ユーザー・グループのメンバーが同じユーザー・グループの他のメンバーと通信することができる。例えば、閉鎖的ユーザー・グループが別の国の軍人グループであったり、別の国の緊急出動要員グループであったりする。

＜その他の実施の形態＞

これまでの説明から、前述の実施の形態は本発明を実施する１つの方法であるに過ぎないことが明らかであろう。本発明の範囲内でその他の多くの代案が可能であることが専門家には明白であろう。

例えば、記載した衛星や衛星の軌道数は単なる一例であるに過ぎない。より少数の静止衛星または高度がより高い軌道の衛星を使用することも可能であり、またはより多数の地球低軌道（ＬＥＯ）衛星を使用することも可能であろう。同様に、中間軌道内の異なる数の衛星を使用することもできよう。

ＴＤＭＡを適切な接続プロトコルとして記載してきたが、本発明は符号分割多元接続（ＣＤＭＡ）または周波数分割多元接続（ＦＤＭＡ）のような他の接続プロトコルにも充分に適用できる。

本発明の原理を衛星通信システムに適用するものとして想定してきたが、（例えばＧＳＭのようなディジタル地上セルラー・システムの）他の通信システムに本発明を利用することも可能である。

便宜上、端末機２を示すのに前述の説明では“移動体”という用語を用いてきたが、この用語は携帯または手持ちの端末機に限定されるものではなく、例えば船舶や航空機、または陸上車両に実装する端末機をも含むことが理解されよう。同様に、本発明を完全に移動不能である、ある種の端末機２とともに実施することも可能である。

全ての端末機２の詳細データを記憶する単一の中央データベース局１５を備える代わりに、同様の詳細データをホーム・ゲートウェイ８に記憶して、全ての端末機をそのホーム・ゲートウェイ８に登録することもできよう。

同様に、上記の実施の形態では中央データベース局１５はＧＳＭシステムのホーム・ロケーション・レジスタ（ＨＬＲ）として機能し、市販のＨＬＲハードウェアを使用して装備してもよく、かつ各地上局６内のデータベースはビジティング・ロケーション・レジスタ（ＶＬＲ）の態様で機能し、同様に市販のＧＳＭハードウェアを使用してもよいが、様々なユーザーに関する情報を幾つかの異なるデータベース間で配分することも可能であることが理解されよう。例えば、物理的に異なる位置に各々の閉鎖的ユーザー・グループ毎に１つのデータベースを備えることもできよう。

同様に、前述の実施の形態では直接送信システムに記載されているが、本発明は一方の記憶のために当事者がメッセージを送信して、これが記憶され、その後で他の当事者に配送または転送されるような蓄積・交換通信システムにも適用できることが明白であろう。

このような蓄積・交換システムの一例は、例えばコンピュサーブ（商標）またはＭＣＩ（商標）によって提供されるタイプのＥ－メールである。その他の例にはインターネットであり、これは公知のように、高速パケット通信リンクのバックボーンによって相互接続され、公衆通信網またはその他の回線網を経て世界中のほとんどの地点からファイル伝送するためにアクセス可能である多数のホストコンピュータ・サイトから構成されている。

この種類の実施の形態では、中央データベース局１５は双方の端末機に同時に鍵を配分する必要はなく、送信側の端末機への部分鍵の配分は、暗号化された形式で記憶されるデータ・ファイルの送信の時点で行われ、また受信側の端末機への部分鍵の配分は実質的に後の時点で行われてもよい。例えば、受信側の端末機が回線網に接続される次の機会、および（または）受信側の端末機がホストコンピュータ内の中間記憶装置からファイルをダウンロードしたい次の機会である。

上記の実施の形態は音声通信に関して説明しているが、本発明をどのような種類のデータの暗号化にも適用でき、それに限定されるものではないが、特に画像データ、ビデオデータ、テキストファイル等にも適用できることが当然理解されよう。

本発明の様々な構成要素の地理的な配置は重要ではなく、様々な国内管轄区域内に上記の実施の形態のシステムの様々な部品を装備してもよいことが理解されよう。本発明は疑念の余地なく、本発明の概念に寄与する通信装置、またはシステムのどの部品もしくは構成要素にも拡張できる。

本発明の前述の、およびその他の全ての変化形、修正および改良は本発明の範囲内に含まれることを意図するものである。

上記の第４の実施の形態では、エアインターフェース暗号化用に使用されるものと同じ端末機鍵K_iがセキュリティ端末機間暗号化用に使用されているが、必ずしもそうである必要はないことは明かである。それぞれの端末機が２つの異なる端末機鍵を記憶することができよう。すなわち１つの端末機鍵はエアインターフェース暗号化用であり、もう１つは端末機間暗号化用である。この場合は、従来のエアインターフェース暗号化で使用されるものとは別個の認証用中央データベースを端末機間の暗号化鍵配分用に備えることもできよう。

前述の実施の形態では、ＧＳＭシステムのエアインターフェース暗号化用に使用される同じ（Ａ５）暗号化アルゴリズムを端末機間の暗号化にも使用することが提案されているが、異なる暗号化方式を採用してもよいことが明らかであろう。その場合は、端末機は第４の実施の形態で使用するための２つの異なる暗号化段を含んでいよう。更に、複数の閉鎖的ユーザー・グループがある場合は、それぞれの閉鎖的ユーザー・グループは異なる暗号を使用できよう。

前述の実施の形態で、ゲートウェイ８は実際にはゲートウェイの機能を実行する補足的な動作制御プログラムを備えることによってＩＳＣ、または交換または移動体切換えセンター（ＭＳＣ）に内蔵されていてもよい。

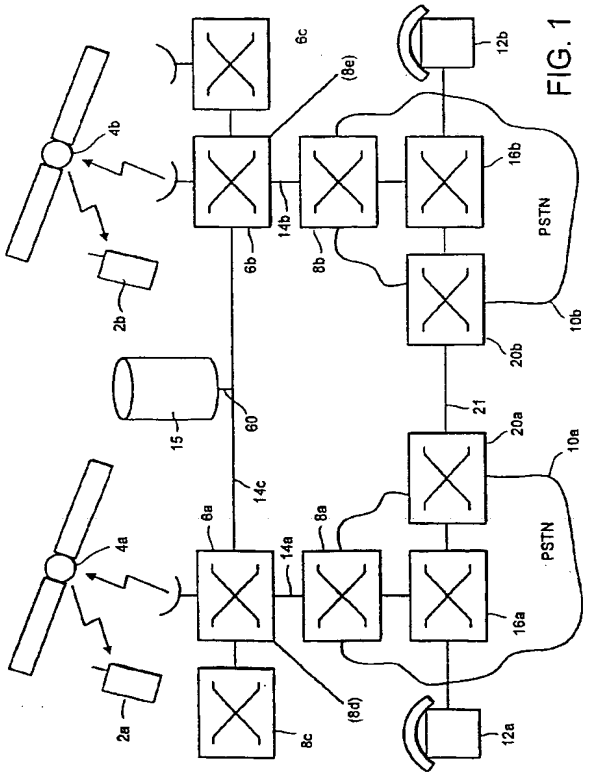
前述の実施の形態では専用の地上回線が記載されており、これが好適である。しかし、例えば専用回線を使用できない場合、または交信状態に対処するために暫定的に付加的な容量を要する場合は、ＰＳＴＮまたはＰＬＭＮリンクを使用しても構わない。

ゲートウェイ８内の記憶装置は、信号線を介して接続されていれば、その他の構成部品と物理的に同一の位置に配置する必要はないことは勿論である。

前述の実施の形態では、“大域的”という用語が用いられ、衛星システムが地球の全領域、またはほとんどの部分をカバーすることが好適ではあるものの、本発明はカバー領域がより限定された（例えば１つ以上の大陸）同様のシステムにも拡張できる。

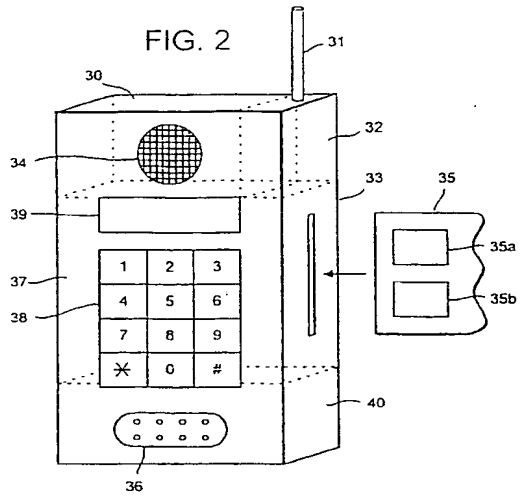
前述の実施の形態では二重通信システムを記載しているが、本発明はポイント・ツー・マルチポイント、もしくは放送システムのような単信（１方向）送信システムにも適用できることが明白であろう。

【図１】



【図２】

FIG. 2



【図３】

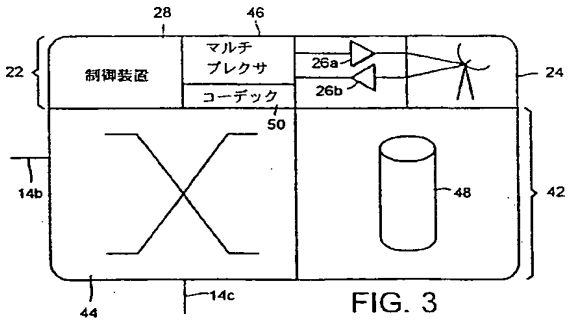


FIG. 3

【図４】

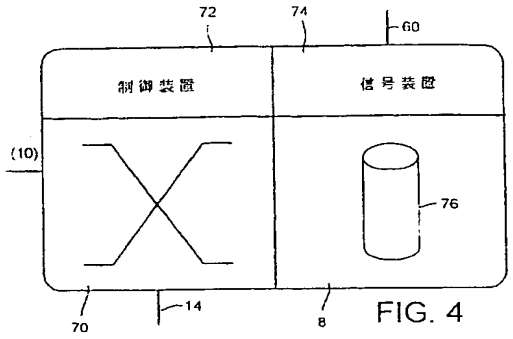


FIG. 4

【図５】

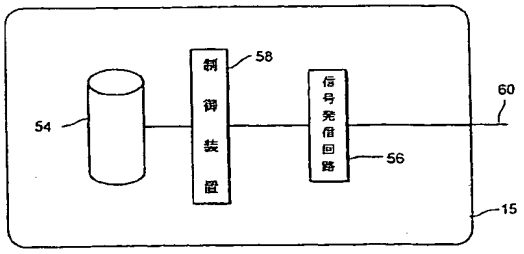


FIG. 5

【図６】

54

識別名#	鍵 Ki	状態	位置	移動ノード	利用？	ホーム
00001	K_A	局所内	46°, 35°	6a	Y	8a
00002	K_B	大域的	71°, 27°	6b	Y	8b

FIG. 6

【図８】

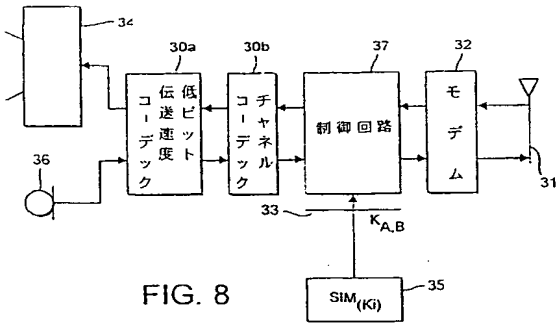
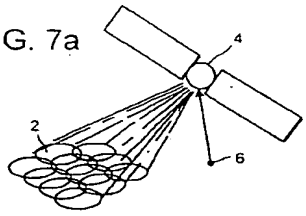


FIG. 8

【図７】

FIG. 7a



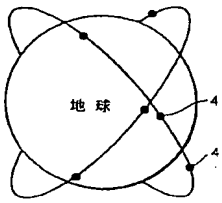


FIG. 7b

【図９】

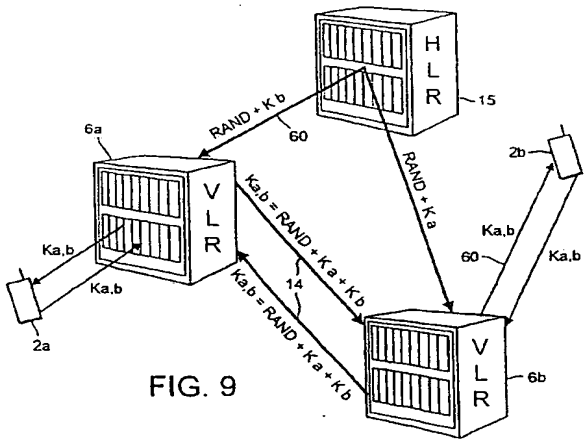


FIG. 9

【図１０】

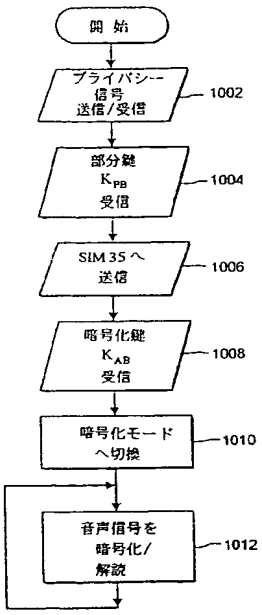


FIG. 10a

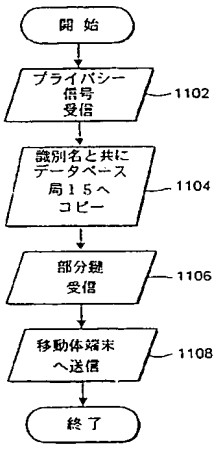


FIG. 10b

【図１０】

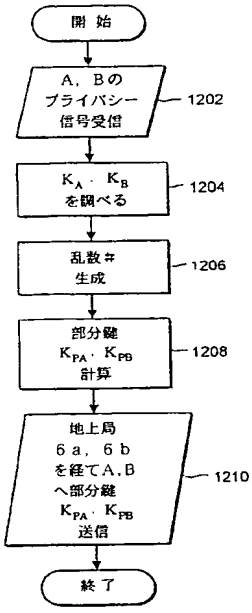


FIG. 10c

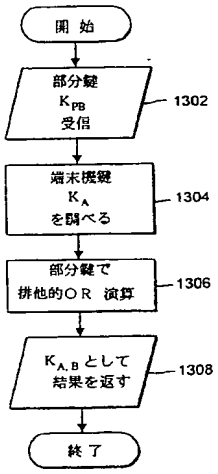


FIG. 10d

【図１１】

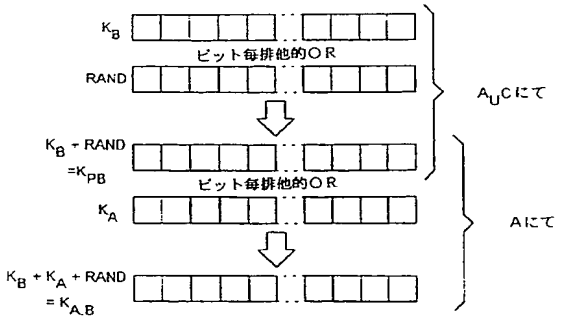


FIG. 11a

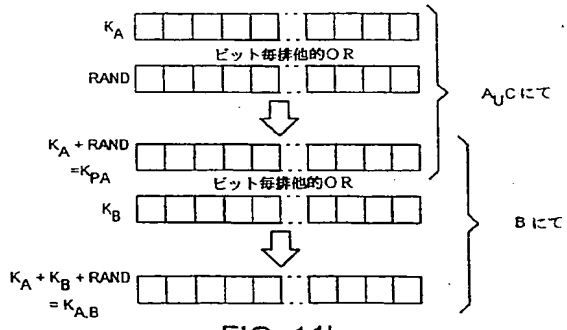


FIG. 11b

【図１２】

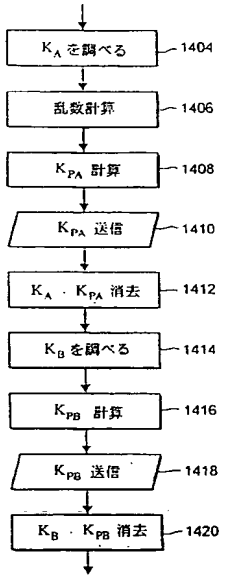


FIG. 12

【図１３】

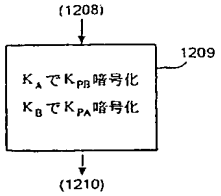


FIG. 13a

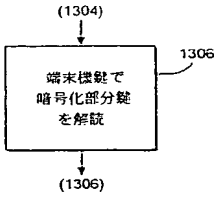


FIG. 13b

【図１４】

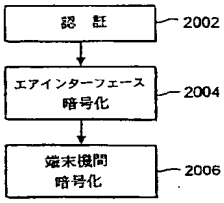


FIG. 14

【図１５】

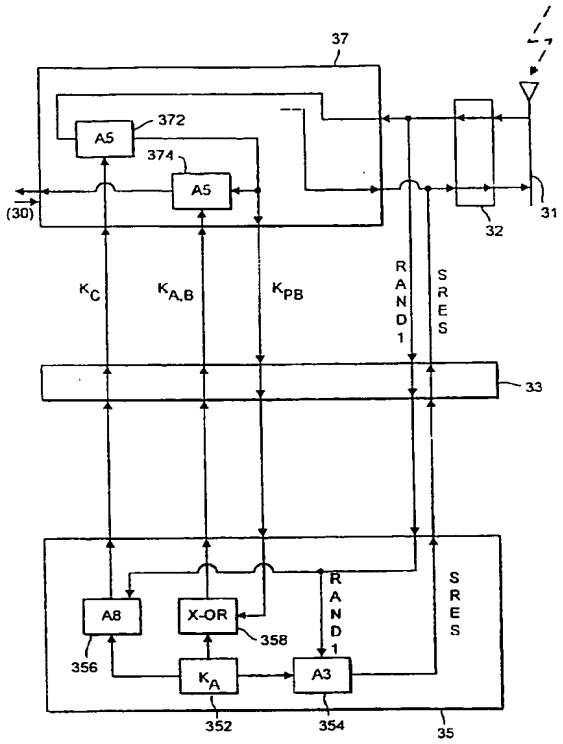


FIG. 15a

【図１５】

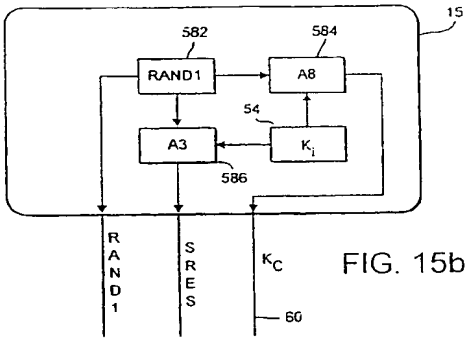


FIG. 15b

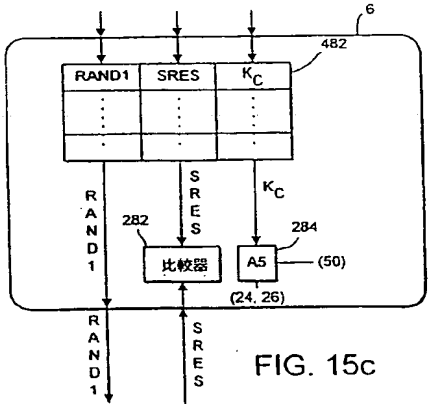


FIG. 15c

【図１６】

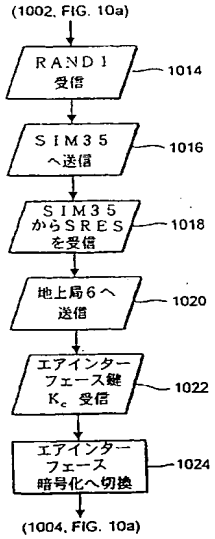


FIG. 16a

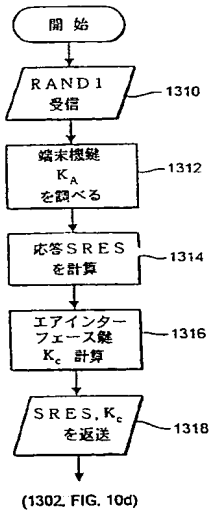


FIG. 16d

【図１６】

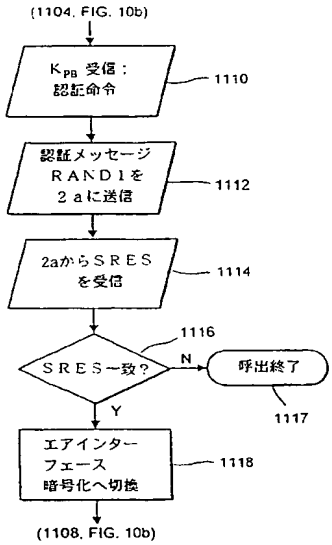


FIG. 16b

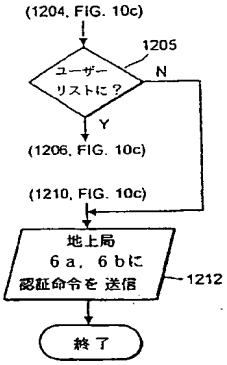


FIG. 16c

フロントページの続き

(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＺ，ＵＧ)，ＵＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＥ，ＨＵ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＴＪ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＳ，ＵＺ，ＶＮ

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna ..al Application No
PCT/GB 97/01407

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 688 140 A (INFORMATIKZENTRUM DER SPARKASS) 20 December 1995 see column 2, line 53 - line 58 see column 3, line 24 - line 30 see column 3, line 53 - column 4, line 4 see column 5, line 10 - last line ---	1,2,5, 13-15
X	CAMPANINI ET AL. : "PRIVACY, SECURITY AND USER IDENTIFICATION IN NEW GENERATION RADIOMOBILE SYSTEMS" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS, 30 June 1987, VENICE (IT), pages 152-164, XP002040784 see page 159, line 9 - page 160, line 21 --- -/--	1,5, 13-15, 17,29

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 September 1997	29. 09. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna...al Application No
PCT/GB 97/01407

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DIFFIE ET AL.: "MULTIUSER CRYPTOGRAPHIC TECHNIQUES" AFIPS CONFERENCE PROCEEDINGS OF NATIONAL COMPUTER CONFERENCE, vol. 45, June 1976, pages 109-112, XP002040785 see page 110, left-hand column, line 19 - line 36 ---	1,13
X	EP 0 365 885 A (MOTOROLA) 2 May 1990 see abstract see column 7, last paragraph ---	25
A	FR 2 608 338 A (ELECTRONIQUE SERGE DASSAULT) 17 June 1988 see page 3, line 21 - line 33 see page 4, line 30 - line 34 see page 9, line 18 - line 32 ---	35
A	AREND VAN DER P C J: "SECURITY ASPECTS AND THE IMPLEMENTATION IN THE GSM-SYSTEM" PROCEEDINGS OF DIGITAL CELLULAR RADIO CONFERENCE, 12 October 1988, pages 4A/1-4A/07, XP000618482 cited in the application see page 4A2, last paragraph - page 4A3, line 20 -----	1,13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna ..al Application No
PCT/GB 97/01407

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0688140 A	20-12-95	NONE	
EP 365885 A	02-05-90	AT 127974 T	15-09-95
		AU 628081 B	10-09-92
		AU 4169389 A	03-05-90
		CA 1338020 A	30-01-96
		CN 1042278 A,B	16-05-90
		DE 68924234 D	19-10-95
		DE 68924234 T	02-05-96
		EG 19299 A	29-06-95
		ES 2076945 T	16-11-95
		HK 113996 A	05-07-96
		HR 940222 A	30-04-96
		JP 2179035 A	12-07-90
		KR 9707988 B	19-05-97
		NO 177480 B	12-06-95
		OA 9055 A	31-03-91
		PL 167049 B	31-07-95
		PT 92102 B	31-05-96
		TR 25340 A	01-03-93
		US 5410728 A	25-04-95
FR 2608338 A	17-06-88	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)